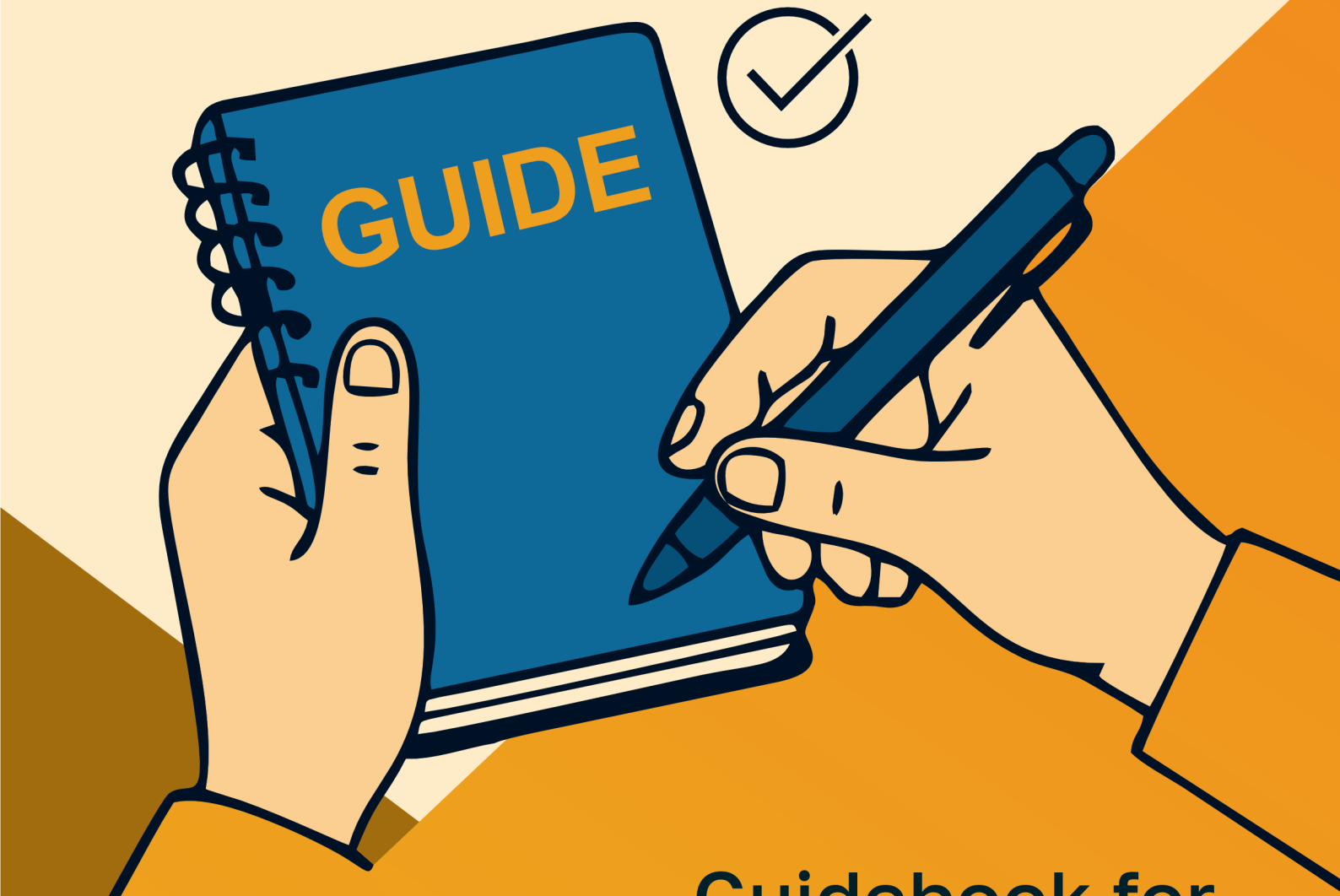
EUComplianceM4UA

Co-funded by the European Union



Guidebook for Master's Students

COMPLIANCE MANAGEMENT

EUComplianceM4UA

Co-funded by the European Union

Guidebook for Master's Students

COMPLIANCE MANAGEMENT

Co-funded by the European Union

EUComplianceM4UA

UDC 005.35:005.334(075.8)

Compliance Management: Guidebook

Editorial Team:

Dr. prof. ***Ali Arnaout, Dr. Anna Fomenko,*** Hochschule Wismar – University of Applied Sciences Technology, Business and Design (Germany)

Reviewers:

Oleksandra VAGONOVA – Doctor of Economic Sciences, Professor, Head of the Department of Applied Economics, Entrepreneurship, and Public Administration, Dnipro University of Technology, Dnipro, Ukraine

Ivan KRIUKOV **–** Anti-Corruption Compliance Officer, Head of the Economic Security Division of the Security Department, JSC "Energy Company of Ukraine"

The Guidebook, as an official educational e-learning resource within the EUComplianceM4UA Project, was approved by the Meetings of the Academic council of Central Ukrainian National Technical University (minutes №1, 29.08.2025) and is recommended for use in the educational process at all partner universities.

Project: EUComplianceM4UA, Implementation of the European Approach of Compliance Management in Higher Education in Ukraine, №101179706

Project type: ERASMUS-EDU-2024-CBHE-STRAND-1 ERASMUS-LS

Project website: https://eucompliancem4ua.eu/

Year of publication: 2025

Edition: First edition

ISBN: 978-617-8588-17-5

Every effort has been made to verify the accuracy of the information contained in this report. All information was believed to be correct as of October 2025. Nevertheless, cannot accept responsibility for the consequences of its use for other purposes or in other contexts.

This publication was produced as part of the EUComplianceM4UA project, which is co-funded by the European Union. The guidebook may be shared and quoted with proper attribution, but it may not be altered, adapted, translated, or redistributed in modified form without prior permission. Quotation is permitted with appropriate acknowledgement. For permission requests regarding adaptations or derivative works, please contact the EUComplianceM4UA project team https://eucompliancem4ua.eu/ .

Disclaimer

The creation of this communication has been funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor the European Education and Culture Executive Agency (EACEA) can be held responsible for them.

@Ali Arnaout, Anna Fomenko,
Iryna Androshchuk, Maryna Vasylieva, Oleksandra Gron, Iuliia Dudnieva,
Olha Lunhol, Olena Magopets, Iryna Murashko, Iryna Murenets, Halyna Nazarova,
Yehor Nazymko, Roman Nesterenko, Pavlo Otenko, Andrii Pastushenko,
Tetiana Ponomarova, Marharyta Chepeliuk, Viktoriia Chobitok, Volodymyr Shalimov,
Nataliia Shalimova, Iryna Shteimiller, Olena Yakovenko, Olena Iarmosh.
@EUComplianceM4UA

Co-funded by the European Union

EUComplianceM4UA

Table of Contents

Acknowledgements, Contributors, Presentation of the Project & Disclaimer **6**

Acknowledgements 6

Contributors 7

Presentation of the Project 8

Introduction 10

Purpose of this Book 10

How to use Guidebook 10

Overview of the Guidebook 12

Relevance of Compliance Management for Master's students 13

Learning Outcomes Recap 15

Glossary of Key Terms **17**

Chapters of the Guidebook **19**

Chapter 1: Foundations and Philosophy of Compliance Management 20

Chapter 2: Business Ethics, Integrity & Compliance 33

Chapter 3: Legal Frameworks and International Compliance Standards 75

Chapter 4. Compliance Management Systems: Elements and Functions 91

Chapter 5: Compliance Organizations, Corporate Culture & Leadership (CECO) 105

Chapter 6: Human Resource Management for Compliance (eg HSEQ) 117

Chapter 7: Compliance Communication and Whistlblowing 154

Chapter 8: Compliance Risk Management 175

Chapter 9: Anti-Corruption Policy and Corporate Compliance 190

Chapter 10: Evaluating the Effectiveness of a Compliance Management. Reporting 209

Chapter 11: Compliance Management for ESG Goals, Corporate Sustainability and Social Impact 252

Chapter 12: Compliance Management IT Solutions (Data Protection, AI, Cybersecurity) 270

Chapter 13: Compliance in Multinational Corporations. Third-Party & Supply Chain Compliance 285

Knowledge Quality Self-Assessment Checklist **301**

How to Apply Your Knowledge? **303**

Recommended Resources **305**

Appendices **307**

ACKNOWLEDGEMENTS, CONTRIBUTORS, PRESENTATION OF THE PROJECT

Acknowledgements

Guidebook, «Compliance Management: Masters Student Guidebook,» is a tangible outcome of the collaborative efforts undertaken within the framework of the Erasmus+ Capacity Building project «EUComplianceM4UA – Implementation of the European Approach of Compliance Management in Higher Education in Ukraine» (Project number: 101179706). We extend our sincere gratitude to the European Education and Culture Executive Agency (EACEA) for their invaluable support and funding under the ERASMUS-EDU-2024-CBHE call, specifically ERASMUS-EDU-2024-CBHE-STRAND-1. This project would not have been possible without the dedication and expertise of the coordinating institution, Hochschule Wismar – University of Applied Sciences Technology, Business and Design, and all partner institutions:

> Coordinating Institution: Hochschule Wismar – University of Applied Sciences Technology, Business and Design (Germany)

> Universidade Portucalense Infante D Henrique-Cooperativa de Ensino Superior CRL (Portugal)

> Vysoka Skola Chemicko-Technologicka v Praze (Czechia)

> Wyzsza Szkola PrzedsiebiorczosclI Administracji w Lublinie (Poland)

> Central Ukrainian National Technical University (Ukraine)

> Izmail State University of Humanities (Ukraine)

> Simon Kuznets Kharkiv National University of Economics (Ukraine)

> Donetsk State University of Internal Affairs (Ukraine)

> V. N. Karazin Kharkiv National University (Ukraine)

> NGO “Professional Network of Research and Higher Education Managers in Ukraine (Ukraine)

Their commitment to enhancing compliance education and fostering academic integrity has been instrumental in the development of this resource.

The editors’ team would like to thank the supporting organisations and NGO in Europe and Ukraine, such as DICO (Germany), PwC Germany, Daimler Track (Germany), DUAG (Germany), PINKTUM (Germany), Carnival Corporation (USA), YouControl (Ukraine), Business-format Group (Ukraine), for their support in the process of providing educational meetings, briefings, workshops, and for the process of communication with stakeholders.

Co-funded by the European Union

Contributors

The idea for this guidebook emerged in the course of implementing the **EUComplianceM4UA** project through ongoing academic cooperation, professional dialogue, and the exchange of ideas among partner higher education institutions. The publication reflects the shared efforts of the consortium to develop a comprehensive and practice-oriented resource on compliance management for higher education and professional training contexts.

The original concept of the guidebook, including its thematic vision and structural framework, Acknowledgements, Presentation of the Project, Introduction, Glossary of Key Terms, Knowledge Quality Self-Assessment Checklist, How to Apply Your Knowledge, Recommended Resources, and Appendices was developed by ***Ali Arnout*** and ***Anna Fomenko*** *(*Hochschule Wismar – University of Applied Sciences Technology, Business and Design, Germany)*,* whose contribution laid the foundation for the collaborative work of all chapter authors.

The guidebook brings together contributions from academic staff of partner universities, with individual chapters prepared by the following authors:

Chapter 1. Foundations and Philosophy of Compliance Management. V. N. Karazin Kharkiv National University (Ukraine) - *Viktoriia Chobitok, Roman Nesterenko,* Hochschule Wismar – University of Applied Sciences Technology, Business and Design (Germany) – *Ali Arnaout*

Chapter 2. Business Ethics, Integrity & Compliance. Donetsk State University of Internal Affairs (Ukraine) - *Yehor Nazymko, Volodymyr Shalimov;* Hochschule Wismar – University of Applied Sciences Technology, Business and Design (Germany) **–** *Ali Arnaout, Anna Fomenko*

Chapter 3. Legal Frameworks and International Compliance Standards. Simon Kuznets Kharkiv National University of Economics (Ukraine) - *Marharyta Chepeliuk, Pavlo Otenko*

Chapter 4. Compliance Management Systems: Elements and Functions. Izmail State University of Humanities (Ukraine) - *Olena Yakovenko, Iryna Murashko*

Chapter 5. Compliance Organisations, Corporate Culture & Leadership (CECO). V. N. Karazin Kharkiv National University (Ukraine) - *Iuliia Dudnieva, Maryna Vasylieva, Iryna Shteimiller*

Chapter 6. Human Resource Management for Compliance (e.g. HSEQ). Central Ukrainian National Technical University (Ukraine) - *Olena Magopets, Nataliia Shalimova, Iryna Androshchuk*

Chapter 7. Compliance Communications & Whistleblowing. Central Ukrainian National Technical University (Ukraine) - *Nataliia Shalimova, Olena Magopets, Iryna Androshchuk*

Chapter 8. Compliance Risk Management. Izmail State University of Humanities (Ukraine) - *Olena Yakovenko, Iryna Murashko*

Chapter 9. Anti-Corruption Policy and Corporate Compliance. Donetsk State

University of Internal Affairs (Ukraine) - *Yehor Nazymko, Tetiana Ponomarova*

Chapter 10. Evaluating the Effectiveness of Compliance Management. Reporting. Central Ukrainian National Technical University (Ukraine) - *Halyna Nazarova, Nataliia Shalimova*

Chapter 11. Compliance Management for ESG Goals, Corporate Sustainability and Social Impact. Simon Kuznets Kharkiv National University of Economics (Ukraine) - *Olena Iarmosh, Iryna Murenets*

Chapter 12. Compliance Management IT Solutions (Data Protection, AI, Cybersecurity). Donetsk State University of Internal Affairs (Ukraine) - *Olha Lunhol*

Chapter 13. Compliance in Multinational Corporations, Third-Party & Supply Chain Compliance. Simon Kuznets Kharkiv National University of Economics (Ukraine) - *Oleksndra Gron, Andrii Pastushenko*

The guidebook is therefore the result of a joint intellectual effort combining institutional expertise, thematic specialisation, and a shared commitment to strengthening compliance education and culture.

Presentation of the Project

Guidebook is a direct output of the Erasmus+ Capacity Building project «EUComplianceM4UA – Implementation of the European Approach of Compliance Management in Higher Education in Ukraine» (Project number: 101179706). This initiative, launched under the ERASMUS-EDU-2024-CBHE call, specifically ERASMUS-EDU-2024-CBHE-STRAND-1, represents a significant collaborative effort between 4 EU universities and 5 Ukrainian universities. Further information about the project can be found on its official website: https://eucompliancem4ua.eu/.

The project's central focus is the implementation of the European approach to Compliance Management, with a strategic aim to elevate academic integrity, international management, entrepreneurship, business ethics, and legal aspects in less experienced Ukrainian HEIs. The goal is to enhance teaching and assessment mechanisms for Higher Education Institutions (HEIs), focusing on quality assurance, management, anti-bribery, and innovation in accordance with EU Compliance standards.

Specifically, the project and, by extension, this Guidebook, address several key objectives:

- Elevating Teaching Methods: The project seeks to significantly improve teaching and assessment mechanisms, quality assurance, management practices, and innovation within Ukrainian HEIs by seamlessly integrating EU Compliance methodologies into their curricula.
- Increasing Accessibility of Compliance Education: A core aim is to enhance both the access to and the quality of Compliance Management education in the fields of entrepreneurship, management, and law within Ukrainian HEIs. This is intended to foster greater adaptability among graduates to the requirements of the European labor market.

- Fostering Employment Stability for Ukrainian University Graduates: By equipping Ukrainian university graduates with essential compliance competencies, the project endeavors to ensure greater stability in their employment opportunities within the broader context of European integration and globalization.
- Empowering Digital Transformation: The initiative actively promotes digital transformation in the teaching of Compliance Management within Ukrainian partner HEIs. This includes the development and utilization of innovative tools such as a futurebook (e-book), podcasts, videos, and gamification solutions, all of which contribute to the modern and effective delivery of educational content. This guidebook, therefore, serves as a cornerstone in achieving these objectives.

INTRODUCTION

Purpose of this Book

Guidebook, «Compliance Management: Masters Student Guidebook,» serves as a comprehensive resource for Master's students navigating the complex and critical field of compliance management. In an increasingly interconnected and regulated global landscape, understanding and implementing robust compliance frameworks are paramount for organizations across all sectors. This book aims to equip future leaders and professionals with the foundational knowledge, practical insights, and critical thinking skills necessary to excel in this dynamic domain.

Guidebook complex compliance concepts into an accessible format, providing Master's students with a robust foundation that aligns with European standards and prepares them for the demands of a globalized professional environment. It is designed not only to impart knowledge but also to foster a proactive and ethical mindset essential for effective compliance management.

This guidebook aims to synthesize comprehensive research on European Union approaches to Compliance Management, with a specific focus on its relevance and application within Ukrainian contexts.

It is designed to provide Master's students with a coherent and structured resource, enhancing their knowledge and practical skills in compliance management through a clear format including keywords, study guidelines, self-assessment questions, and recommended resources.

Developed with guidance from EU partners and approved by Ukrainian Higher Education Institution partners, this guidebook serves as a valuable tool for academic and practical learning in compliance management.

How to use Guidebook

This guidebook is designed to be a practical companion for Master's students, offering a structured approach to understanding and applying compliance management principles. To maximize your learning experience, we recommend the following approach:

Learning Outcomes

Upon engaging with this guidebook, you will be able to:

> Comprehend the foundational concepts and ethical underpinnings of compliance management.

> Identify and analyze the key legal frameworks and international standards governing compliance.

> Understand the practical application of compliance management systems within organizational structures.

- Develop an ethical mindset and appreciate the role of integrity and leadership in fostering a culture of compliance.
- Recognize the interdisciplinary nature of compliance, linking it to human resources, risk management, and IT solutions.
- Evaluate the effectiveness of compliance programs and contribute to their continuous improvement.
- Connect theoretical knowledge to real-world scenarios through case studies and practical exercises.

Key Terms

Throughout this Guidebook, you will encounter essential terminology. A comprehensive "Glossary of Key Terms" is provided at the beginning of the book, offering short definitions of main compliance-related concepts. Familiarizing yourself with these terms will enhance your understanding of the subject matter.

Structure of Each Chapter

Each chapter in this guidebook is meticulously structured to facilitate effective learning and retention. While the introductory chapters (Purpose of this Guidebook, How to Use this Guidebook, Overview of the Guidebook, Relevance of Compliance Management for Master's students, Learning Outcomes Recap) will differ slightly, the core chapters (1-13) will generally follow a specific format.

For ease of use, the guidebook is structured so that each chapter includes:

- Three general learning outcomes that define what the reader should be able to achieve after studying the chapter.
- List of keywords to help focus on the main concepts.
- Key definitions to ensure a clear understanding of the core terminology.
- Theoretical section covering the main approaches, standards, laws, regulations, and recommendations relevant to the topic.
- Outline of the sub-topics addressed in the chapter.
- Information on prominent scholars and researchers who have made significant contributions to the field.
- Practical examples and case studies from both the European Union and Ukraine.
- Short "Case in Point" boxes presenting real-life situations and their practical implications.
- Hands-on exercises to strengthen understanding and application of the material.
- Reflective questions to encourage critical thinking.

- Selection of additional resources for further exploration.
- Tasks and assignments to support independent learning and consolidation of knowledge.

Navigating the Guidebook

We encourage you to use this guidebook actively. Do not hesitate to:

- Refer to the Acronyms list for quick clarification of abbreviations.
- Consult the Glossary whenever you encounter unfamiliar terms.
- Engage with the Practical Exercises to solidify your understanding.
- Reflect on the Target Questions to deepen your critical thinking.
- Explore the Recommended Resources to expand your knowledge beyond the scope of this book.
- This guidebook is a tool for your academic and professional development in compliance management. We hope it serves as an invaluable resource on your journey to becoming a proficient and ethical compliance professional.

Overview of the Guidebook

This guidebook, «Compliance Management: Masters Student Guidebook,» is meticulously structured to provide a comprehensive and practical understanding of compliance management for Master's students. It is designed to be a foundational resource, guiding readers through the theoretical underpinnings, practical applications, and contemporary challenges within the field of compliance. The content is organized into distinct sections, each building upon the previous one to foster a holistic learning experience.

The core chapters cover a wide array of topics:

1. Foundations and Philosophy of Compliance Management: Explores the fundamental concepts and ethical principles that underpin compliance.
2. Business Ethics, Integrity & Compliance: Delves into the crucial intersection of ethical conduct, corporate integrity, and compliance practices.
3. Legal Frameworks and International Compliance Standards: Examines the global and regional legal structures and standards governing compliance.
4. Compliance Management Systems: Elements and Functions: Provides a detailed look at the components and operational aspects of effective CMS.
5. Compliance Organizations, Corporate Culture & Leadership (CECO): Focuses on the role of leadership and organizational culture in fostering compliance.
6. Human Resource Management for Compliance (eg HSEQ): Discusses how HR practices contribute to and support compliance initiatives.
7. Compliance Communications & Whistleblowing: Covers strategies for effective internal and external communication regarding compliance, including whistleblowing

mechanisms.

8. Compliance Risk Management: Addresses methodologies for identifying, assessing, and mitigating compliance-related risks.
9. Anti-Corruption Policy and Corporate Compliance: Explores policies and practices aimed at preventing corruption within organizations.
10. Evaluating the Effectiveness of a Compliance Management. Reporting: Focuses on methods for assessing CMS efficacy and reporting compliance performance.
11. Compliance Management for ESG Goals, Corporate Sustainability and Social Impact: Connects compliance with environmental, social, and governance objectives and broader sustainability efforts.
12. Compliance Management IT Solutions (Data Protection, AI, Cybersecurity): Examines the role of technology in compliance, including data protection, artificial intelligence, and cybersecurity.
13. Compliance in Multinational Corporations. Third-Party & Supply Chain Compliance: Addresses the complexities of compliance in global operations, including managing third-party and supply chain risks.

Beyond the core chapters, the guidebook provides practical guidance on How to apply your knowledge? and How students can link compliance to future jobs, including real job titles and descriptions such as Compliance Officer, Risk Analyst, and Ethics Consultant, along with required skills. The Recommended Resources section offers a curated list of core textbooks, key regulations and guidelines (EU Directives, Ukrainian Laws), useful websites and databases, journals and articles, video lectures, as well as references to the project website and YouTube channel. This comprehensive structure ensures that the «Compliance Management: Master's Student Guidebook» serves as an invaluable, well-rounded resource for Master's students, preparing them for successful careers in the dynamic field of compliance management.

Relevance of Compliance Management for Master's students

Guidebook is specifically designed to enhance students' level of competencies, skills, and employability potential by improving the educational ecosystem for Master's students in alignment with the evolving EU challenges in Compliance Management.

In a globalized and highly regulated business environment, a comprehensive understanding of compliance management is no longer a niche specialization but a fundamental prerequisite for aspiring business leaders. For Master's students, particularly those in fields such as international management, business administration, economics, and law, a strong grasp of compliance principles is essential for navigating the complexities of the modern corporate world and for building a successful and sustainable career. The study of compliance management equips Master's students with the necessary tools to understand and interpret the intricate web of regulatory and legal frameworks that govern international business. This knowledge is critical for ensuring that organizations operate ethically and within the bounds of the law,

thereby avoiding costly penalties, reputational damage, and legal liabilities. As future managers and executives, students will be responsible for making strategic decisions that have far-reaching implications. A solid foundation in compliance will enable them to make these decisions in a manner that is not only profitable but also principled.

Furthermore, compliance management is not merely about adhering to rules and regulations; it is an integrated function that plays a vital role in shaping corporate culture and driving organizational success. By learning about the functional, organizational, and instrumental subsystems of a Compliance Management System (CMS), students will gain insights into how to design and implement effective compliance programs. This includes understanding the importance of a strong ethical culture, effective communication channels, and robust internal controls. These skills are highly valued by employers, as they contribute directly to the long-term sustainability and resilience of the organization.

Finally, the study of compliance management provides Master's students with a distinct competitive advantage in the job market. As organizations face increasing scrutiny from regulators, investors, and the public, the demand for professionals with expertise in compliance is growing rapidly. By developing a strong understanding of compliance, students will be well-positioned to pursue a variety of rewarding career paths, such as Compliance Officer, Risk Analyst, and Ethics Consultant. These roles are not only intellectually stimulating but also offer the opportunity to make a meaningful impact on the ethical conduct and overall success of an organization.

Learning Outcomes Recap

Upon completing Guidebook, Master's students will be able to:

Comprehend the foundational concepts and ethical underpinnings of compliance management:

> Understand the importance of compliance in business operations, the role of ethics in compliance, and the need for a strong compliance culture.

Understand the practical application of compliance management systems within organizational structures:

> Learn how to design, implement, and maintain effective compliance management systems, including risk assessment, monitoring, and reporting.

Develop an ethical mindset and appreciate the role of integrity and leadership in fostering a culture of compliance:

> Understand the importance of leadership in promoting a culture of compliance, and learn how to foster a culture of integrity and ethics within an organization.

Recognize the interdisciplinary nature of compliance, linking it to human resources, risk management, and IT solutions:

> Learn how compliance intersects with other business functions, including HR, risk management, and IT, and understand how to integrate compliance into these areas.

Evaluate the effectiveness of compliance programs and contribute to their continuous improvement:

> Learn how to assess the effectiveness of compliance programs, identify areas for improvement, and develop strategies for continuous improvement.

Articulate the strategic role of compliance in ensuring business sustainability, protecting corporate reputation, reducing risks, and building trust with partners and regulators:

> Understand the strategic importance of compliance in business operations and learn how to communicate the value of compliance to stakeholders.

Identify applicable Ukrainian and international laws and regulations; apply regulatory requirements (anti-corruption, AML, data protection, ESG) and standards (ISO) into business operations and evaluate their implications for corporate strategy:

> Recognize the relevance of Ukrainian and international laws and regulations in compliance management, and learn how to apply these requirements into business operations.

Identify and assess compliance risks relevant to their industry and organizational context using practical risk tools, with the ability to prioritize risks based on potential impact:

> Learn how to identify and assess compliance risks using practical risk tools, and develop the ability to prioritize risks based on potential impact.

Evaluate current policies and culture, recommend practical steps to strengthen compliance and ethics, create clear policies and procedures, and build awareness and a culture that encourages ethical behaviour:

> Understand the importance of policies and procedures in compliance management, and learn how to create clear policies and procedures that promote a culture of ethics and compliance.

Analyse current data protection and cybersecurity measures, apply GDPR and Ukrainian data laws, manage cybersecurity risks, and propose improvements to align with GDPR and local laws:

> Learn how to analyse current data protection and cybersecurity measures, and develop the ability to apply GDPR and Ukrainian data laws to manage cybersecurity risks.

Monitor and evaluate compliance effectiveness, audit tools, and compliance performance indicators, and prepare compliance reports for internal and external stakeholders, recommending corrective actions that prevent recurrence:

> Understand the importance of monitoring and evaluating compliance effectiveness, and learn how to prepare compliance reports and recommend corrective actions.

Demonstrate ethical leadership by fostering a culture of integrity, transparency, and accountability, ensuring the 'tone from the top' is reflected throughout the organisation:

> Understand the importance of ethical leadership in promoting a culture of compliance, and learn how to foster a culture of integrity, transparency, and accountability.

Use compliance strategically to strengthen reputation and growth, and plan long-term compliance strategies:

> Understand the strategic importance of compliance in business operations, and learn how to use compliance to strengthen reputation and growth.

By achieving these learning outcomes, Master's students will be well-prepared to navigate the complex and dynamic field of compliance management and to make a meaningful impact in their future careers.

Compliance
Adherence to all applicable laws, regulations, internal rules, and ethical standards of an organization. (ISO 37301:2021, DICO Glossary)

Compliance Management System (CMS)
A structured framework that helps an organization establish, develop, implement, evaluate, maintain, and improve compliance processes. (ISO 37301:2021)

Compliance Culture
The values, ethics, and behaviors that encourage lawful and ethical conduct throughout an organization. (ISO 37301:2021, DICO Glossary)

Due Diligence
Systematic process of assessing business partners, projects, or activities to prevent legal and compliance risks. (ISO 37301:2021, DICO Glossary)

Risk Assessment
Process of identifying, analyzing, and prioritizing risks that may affect compliance objectives.
(ISO 31000:2018, referenced in ISO 37301)

Internal Controls
Policies and procedures implemented to ensure compliance, detect irregularities, and safeguard integrity. (ISO 37301:2021, DICO Glossary)

Whistleblowing / Reporting Mechanism
Secure and confidential channel for reporting suspected misconduct or compliance breaches. (ISO 37301:2021, DICO Glossary)

Conflict of Interest
A situation where personal interests may improperly influence professional decisions or actions. (DICO Glossary)

Sanctions / Disciplinary Measures
Consequences for violations of compliance obligations, which may include warnings, penalties, or contract termination. (ISO 37301:2021)

Continuous Improvement
Ongoing process of reviewing and enhancing compliance programs and controls. (ISO 37301:2021, PDCA principle)

Accountability
Clear assignment of responsibilities and obligations to ensure compliance at all levels of the organization. (ISO 37301:2021)

Transparency
Open and accessible communication of compliance-relevant information to stakeholders. (DICO Glossary)

Monitoring and Auditing

Regular evaluation of compliance measures to ensure effectiveness and detect shortcomings. (ISO 37301:2021)

Non-Compliance

Failure to meet applicable legal, regulatory, or organizational requirements. (ISO 37301:2021)

Integrity

Acting in an honest, fair, and responsible manner in all business activities. (ISO 37301:2021, DICO Glossary)

Co-funded by
the European Union

CHAPTERS OF THE GUIDEBOOK

Chapter 1: Foundations and Philosophy of Compliance Management

Learning Outcomes

After studying this chapter, learners will be able to:

> Define the concept and purpose of compliance management in modern organizations.

> Identify key elements and functions of a basic compliance management system.

> Explain the role of compliance in ensuring ethical behaviour, transparency, and responsible decision-making.

Key words: compliance management, internal control, ethical standards, corporate governance, compliance system functions, compliance risk, compliance culture.

Main Definitions

Compliance - is a system of organizational, legal and managerial measures aimed at ensuring that an enterprise complies with the requirements of the law, internal regulatory documents, ethical standards and international business norms.

Compliance Management – a structured organisational process that ensures all activities and decisions align with applicable laws, regulations, standards, and ethical principles.

Compliance System – an integrated set of policies, procedures, and controls designed to prevent, detect, and address legal or ethical violations within an organisation.

Standards, Laws, and Regulations

1. International: ISO 37002:2021 Whistleblowing management systems – Guidelines; ISO 37301:2021 Compliance management systems - Requirements with guidance for use; ISO 37303:2025 Compliance management systems - Guidance for competence management; ISO 31000:2018 Risk management – Guidelines; ISO 45001:2018 Occupational health and safety management systems - Requirements with guidance for use; ISO 9001:2015 Quality management systems – Requirements; ISO 14001:2015 Environmental management systems - Requirements with guidance for use

2. European Union (EU): Directive 2000/78/EC of 27 November 2000 Establishing a general framework for equal treatment in employment and occupation*;* Regulation (EU) 2016/679 of 27 April 2016 General Data Protection Regulation (GDPR) – On the protection of natural persons with regard to the processing of personal data; Directive (EU) 2019/1937 of 23 October 2019 On the protection of persons who report breaches of Union law (Whistleblowing Directive); Directive (EU) 2022/2464 of 14 December 2022 Corporate Sustainability Reporting Directive (CSRD)

3. Ukraine: Labour Code of Ukraine; Law of Ukraine "On Prevention of Corruption"; Law of Ukraine "On Occupational Safety"; Law of Ukraine "On Ensuring Equal Rights and Opportunities for Women and Men"; Law of Ukraine "On Professional Development of Employees"; Order of the National Agency on Corruption Prevention (NACP) No. 127/20 of April 2, 2020 "On Approval of the Requirements for the Protection of Anonymous Communication Channels for Reporting Possible Facts of Corruption or Corruption-Related Offences"

List of Subchapters

1.1 Philosophy and Evolution of Compliance Management

1.2 The Concept and Goals of Compliance Management

1.3 Principles and Functions of Compliance Management

1.4 Main Domains of Compliance Management

1.5 International Perspectives on Compliance Management

1.6 Development of Compliance Management in Ukraine

1.1 Philosophy and Evolution of Compliance Management

The compliance management philosophy is formed at the intersection of legal norms, ethical principles and management practices. It reflects not only the technical side of monitoring compliance with legislation and internal company policies, but also a deep worldview approach to ensuring trust, transparency and business responsibility. In today's conditions of globalization, digitalization and the growth of corporate social responsibility, compliance acquires the status of not just a control tool, but a kind of management philosophy that determines the vector of company development in the long term.

The basis of the compliance philosophy are ethical principles that ensure harmony between the commercial interests of the company and social values. The ethical dimension of compliance involves not only avoiding violations of the law, but also voluntary adherence to high standards of behavior, justice, honesty and decency in relations with partners, clients and state institutions.

From a philosophical point of view, compliance is a manifestation of deontological ethics - the fulfillment of rules and obligations regardless of the benefit that may arise from their violation. This approach allows us to consider compliance management as part of a corporate culture aimed at forming a reputation for responsible business.

The modern philosophy of compliance goes far beyond the control of legal risks and encompasses the values of sustainable development. It involves a balance between economic, social and environmental aspects of the enterprise's activities. From a philosophical perspective, compliance becomes a guide to achieving harmony between

business and society, contributing to minimizing negative environmental impacts, protecting employee rights and developing corporate social responsibility.

The philosophy of compliance contributes to the formation of a sense of involvement in corporate values and an understanding of one's own responsibility for the company's reputation among employees. This, in turn, increases the business's resilience to external challenges and strengthens its competitive advantages (Table 1.1).

Table 1.1 Ethics & Compliance Philosophy

Ethics & Compliance Philosophy		
"Doing the Right Things…"	**"In the Right Way..."**	**"For the Right Reasons…"**
- Complying with the Laws, Regulations and Company Policies - Treating each other with respect - Focusing on the top priority issues - Self-Governing - Prevent / Detect / Respond / Correct	- By Listening To Others - At all Levels - Headquarters and Other Locations - Through Effective Training - Sharing "Lessons Learned" and "Near Misses"	- As Required by Law & Regulations - Many Benefits Beyond Risk Reduction or Legal Issues - It is the Right Thing to Do - It is Who We Are

Source: Prof. Dr. Ali Arnaout, Lecture Materials (used with permission)

The philosophy of compliance management reflects the transition from a narrow interpretation of compliance as a control tool to its understanding as a comprehensive management concept. It is based on ethical principles, an orientation towards trust and legitimacy of business, the integration of sustainable development goals and the formation of a strong corporate culture.

In this approach, compliance becomes not only a means of reducing risks, but also a strategic resource that ensures long-term competitiveness and sustainable development of the enterprise

Compliance management has developed gradually, reflecting global changes in regulation and corporate governance. Its early foundations appeared in the 1950s–1970s in the United States, where the Bank Secrecy Act (1970) introduced mandatory monitoring of financial transactions to prevent money laundering.

A major shift occurred in 1977 with the adoption of the Foreign Corrupt Practices Act (FCPA), which prohibited bribery of foreign officials and promoted ethical business conduct. Over time, many countries introduced similar rules and corporate ethics frameworks.

In the 1990s-2000s, compliance became a core element of corporate governance. Companies developed codes of conduct, internal standards and control procedures. The Sarbanes-Oxley Act (2002) strengthened executive responsibility for financial reporting, while European states advanced their own anti-corruption and governance reforms.

The 2010s brought the globalisation and digitalisation of compliance. Key developments included the EU General Data Protection Regulation (GDPR, 2016) and the introduction of international standards such as ISO 19600 and ISO 37001, expanding compliance to areas like data protection, environmental responsibility and social governance.

In the 2020s, compliance has become integrated into strategic management and the ESG agenda. New domains such as IT compliance and cybersecurity have gained importance. The publication of ISO 37301:2021 marked the transition to a certifiable international standard for compliance management systems, reinforcing compliance as a structured and measurable organisational function.

1.2 The Concept and Goals of Compliance Management

Over the years, Compliance Management has evolved from being seen as a “box-ticking exercise” to becoming a strategic pillar of governance. The “old school”-thinking views compliance as liability-driven, reactive, externally regulated, adversarial, and defensive. In contrast, the “new school” modern view has transformed compliance into a reputation-driven, preventive approach oriented towards internal self-governance, cooperation, transparency, and open corrective measures. This new school approach reduces firefighting and turns compliance into a management capability and a source of competitive advantage.

Scholars and international organisations offer a variety of perspectives on the essence of compliance management. According to the International Compliance Association (2022), compliance management is understood primarily as an organisational process that ensures adherence to regulatory requirements and principles of responsible business conduct. A broader institutional view is presented by DiMaggio (2016), who interprets compliance as a mechanism that helps organisations adapt to an increasingly complex regulatory environment. Other researchers, such as Aguilera and Cuervo-Cazurra (2019), emphasise the strategic nature of compliance, describing it as a system of practices that supports both legal conformity and long-term organisational sustainability. Parker (2015) highlights the ethical dimension, framing compliance as a form of internal self-regulation aimed at promoting lawful and responsible behaviour. These scholarly interpretations align with the guidelines of international standards, such as ISO 37301, which defines compliance as meeting an organisation’s binding and voluntary obligations, supported by a culture of integrity embedded throughout organisational structures and processes.

The main goal of compliance management is to minimize legal, financial and reputa-

tional risks that arise when doing business.

The main objectives of compliance management typically include:

- ensuring that the organisation consistently meets its legal, regulatory and internal compliance obligations;
- preventing, detecting and responding to risks of non-compliance, including corruption, fraud and other forms of misconduct;
- protecting the interests of shareholders, employees, clients and business partners by reducing legal, financial and reputational risks;
- enhancing transparency, accountability and trust in organisational processes and decisions;
- promoting a culture of integrity and establishing clear ethical standards for employee behaviour.

Thus, compliance is a tool aimed not only at control, but also at developing a company based on the principles of honesty and sustainability.

1.3 Principles and Functions of Compliance Management

An effective compliance management system is based on a number of fundamental principles (ISO 37301):

- Integrity – Acting with honesty and fairness in every decision and process.
- Good Governance – ensuring responsible, transparent, and effective management of the organization.
- Proportionality – designing compliance measures that match the organization's size, structure, and level of risk
- Transparency – communicating clearly and openly with stakeholders about compliance matters
- Accountability – taking responsibility for actions and ensuring oversight at every level
- Sustainability – building compliance practices that endure and continuously improve over time

Compliance management functions go beyond simple monitoring of compliance with rules: they shape a culture of honest business conduct, strengthen stakeholder trust and ensure the company's sustainable development.

The control function focuses on monitoring adherence to laws, regulations and internal policies. It includes regular checks, internal audits and documentation of findings to ensure that management receives timely and accurate information about potential violations.

The preventive function aims to identify risks at an early stage and reduce the likelihood of breaches. This involves developing internal policies, codes of conduct and anti-corruption programmes that create clear behavioural standards for employees.

The advisory and methodological function provides guidance to staff and managers on compliance-related issues. It includes consulting on complex ethical or legal questions and preparing methodological materials that support consistent decision-making.

The educational and training function ensures that employees understand compliance expectations. Through training sessions, workshops and awareness activities, organisations build a corporate culture based on transparency, accountability and respect for rules.

The coordination function facilitates cooperation across different departments. Compliance officers work with legal, security, internal audit and other units to integrate compliance into the overall risk management system and to maintain effective communication with regulators.

The analytical function involves collecting and analysing data on violations, trends and potential threats. Based on this information, compliance specialists prepare reports, forecasts and recommendations to improve internal controls.

The regulatory function relates to creating and updating internal standards, rules of conduct and procedures such as conflict-of-interest management. Compliance also contributes to shaping broader corporate policies that support sustainable and responsible behaviour.

The reputational function helps organisations maintain trust among stakeholders by ensuring transparency and timely responses to incidents. Effective compliance reduces reputational risks and reinforces confidence in the company's integrity.

Finally, the anti-crisis function prepares organisations to respond to serious breaches or crisis situations. It includes developing response mechanisms, conducting internal investigations and ensuring that appropriate corrective measures are taken.

Interaction with external auditors, regulatory authorities and the media. Compliance plays the role of a link between the legal department, internal audit and the company's management.

1.4 Main Domains of Compliance Management

Compliance management covers several key domains that reflect the diversity of organisational risks and regulatory expectations. These domains help organisations structure their compliance activities and ensure that obligations are met across different functional areas. The most widely recognized domains include several tasks and examples (Table 1.2).

Table 1.2 Domains of Compliance Management

Compliance Domain	Key Tasks	Examples
Regulatory Compliance	Monitoring legislative and regulatory changes Updating internal procedures Ensuring timely reporting and documentation	Compliance with national labour laws, licensing requirements, industry-specific regulations
Anti-Corruption and Anti-Bribery Compliance	Implementing policies against bribery and improper influence Managing conflicts of interest Establishing reporting and investigation procedures	Anti-bribery controls under the UK Bribery Act, FCPA, ISO 37001
Financial and AML Compliance	Conducting customer due diligence (CDD) Monitoring transactions Reporting suspicious activities	Anti-money laundering procedures in banks; compliance with FATF recommendations
Data Protection and Privacy Compliance	Managing personal data in line with legal requirements Implementing information security controls Conducting data protection impact assessments	GDPR compliance; data breach response protocols
Ethics and Corporate Conduct Compliance	Developing and communicating codes of conduct Managing whistleblowing channels Promoting ethical behaviour and integrity culture	Ethics hotlines, conflict-of-interest declarations, training on ethical dilemmas
Environmental, Social and Governance (ESG) Compliance	Integrating sustainability requirements into operations Ensuring responsible supply chain practices Reporting ESG performance	Compliance with non-financial reporting directives, climate-related disclosures
Operational and Sector-Specific Compliance	Ensuring adherence to technical, safety, and industry standards Managing risks specific to operational processes Conducting regular inspections and certifications	Quality management in healthcare; safety standards in energy and manufacturing sectors

Compliance management is implemented through: internal policies and standards (code of corporate ethics, anti-corruption policy, etc.); internal control system and regular inspections; anonymous reporting mechanisms ("hotline"); personnel training; use of automated monitoring and reporting systems.

1.5 International Perspectives on Compliance Management

The development of compliance management in EU and USA is closely related to the formation of a modern corporate culture, increased regulatory pressure and the globalization of financial markets. The experience of the world's leading economies demonstrates that compliance systems play a key role in preventing corruption, protecting investors' rights, strengthening trust in business and increasing its sustainability. The United States of America is the founder of modern compliance management. The first elements of the system appeared in the 1970s after the adoption of the Foreign Corrupt Practices Act (FCPA, 1977), which obliged companies to prevent bribery of foreign officials. Since then, compliance has become an integral part of corporate governance.

In the 1990s, the Sentencing Guidelines for Organizations (1991) standards were developed, establishing requirements for the creation of effective internal control programs, anti-corruption policies and codes of ethics. Later, the United States increased its emphasis on combating money laundering and terrorist financing (Patriot Act, 2001).

Today, most American corporations have separate compliance departments reporting to the board of directors. Particular attention is paid to data protection, combating fraud, antitrust compliance and ESG standards. In the EU, compliance is developing as a comprehensive and integrated system, closely linked to risk management, corporate governance and regulatory harmonisation. The main priorities include consumer protection, market transparency, and alignment of national legislation with EU-wide standards. Key compliance domains include:

- Data protection, based on the General Data Protection Regulation (GDPR, 2018) – Anti-corruption and anti-money laundering, regulated through the EU AML Directives.
- Competition and antitrust compliance, ensuring fair market practices under EU competition law.

European companies are actively implementing ethical codes, internal audit procedures and whistleblowing mechanisms (anonymous reporting systems). Unlike the US, the EU focuses not only on sanctions, but also on forming a compliance culture within organizations.

Compliance has received separate development in the UK. The UK Bribery Act (2010) introduced some of the world's toughest anti-corruption requirements. The law applies to companies operating not only in the UK but also abroad.

In addition, significant attention is paid to the protection of workers' rights, corporate responsibility and environmental sustainability. British banks and insurance companies have strong compliance control departments that closely interact with government regulators.

In Asian countries, compliance began to actively develop in the 2000s under the influence of globalization and transnational corporations. In Japan, the emphasis is on compliance with labor laws, corporate ethics and investor protection. China is developing its own mechanisms of financial and antitrust regulation, strengthening government control over business. Singapore is considered one of the leaders in Asia due to the creation of an effective system of anti-corruption regulation and transparent corporate governance.

1.6 Development of Compliance Management in Ukraine

Compliance management as a system of risk management and ensuring compliance with legislation, standards and corporate norms in Ukraine began to actively develop relatively recently. Its development is closely linked to the processes of European integration, corporate governance reform, strengthening of anti-corruption policy, as well as the need to increase business transparency for international partners and investors. Compliance management in Ukraine has evolved in several stages. In the early 2000s, the concept was almost absent, and most organisations limited themselves to basic legal functions. First compliance practices appeared mainly through foreign investors who introduced anti-corruption policies, KYC procedures, and internal audit. Between 2010 and 2014, cooperation with the EU and preparation for the Association Agreement stimulated the adoption of European regulatory standards, especially in the financial sector. The National Bank of Ukraine strengthened AML requirements, forming the basis for a more structured approach.

During 2015-2020, the creation of key anti-corruption institutions such as NABU, NAPC and the Specialised Anti-Corruption Prosecutor's Office accelerated the development of corporate compliance programmes. International companies in banking, IT and pharmaceuticals began implementing comprehensive compliance systems. Since 2021, compliance in Ukraine has developed under the influence of digitalisation and wartime conditions. Priority areas now include cybersecurity, data protection, sanctions compliance, ESG requirements and transparency in public procurement. Compliance has become an essential element of sustainable and responsible management across sectors.

Features and challenges of implementing compliance in Ukraine:

- A limited level of legal and ethical awareness within organisations, which affects the understanding of the strategic role of compliance.
- A predominantly formalistic approach in some companies, where compliance policies exist on paper but are not fully integrated into everyday practices.
- A shortage of qualified professionals, particularly compliance officers with relevant international training and practical experience.
- Need to align national practices with European standards, including key EU directives and regulations such as AML frameworks, GDPR requirements, and ESG-related guidelines.

Practical Exercises

Exercise 1 – Exploring ISO 37301:2021 Compliance management systems – Requirements with guidance for use

Open the full text of ISO 37301:2021 Compliance Management Systems. Review the structure of the standard (table of contents only) and complete the following small tasks:

> Identify three sections of the standard that, in your opinion, are the most important for organisations beginning to implement compliance management.
> For each selected section, write one sentence explaining why you consider it important.
> Choose one requirement ("shall" statement) from any clause and summarise it in your own words (2-3 sentences).

Exercise 2 – Analysing Ethical and Compliance Risks

Read the three brief scenarios below and identify the type of compliance risk and the principle of compliance management that is most relevant for addressing it.

Scenarios:

a) A manager informally approves a contract without following the documented internal approval procedure.

b) An employee receives a valuable gift from a supplier during contract negotiations.

c) Customer data is stored without proper access controls.

Questions:

> Which compliance principle (e.g., integrity, transparency, accountability) is violated or at risk?
> What is the potential impact for the organisation?
> What preventive measures could be introduced?

Exercise 3 – Evolution of Compliance Management: Short Analytical Task

Using the historical stages of compliance development presented in Chapter 1, prepare a short-written reflection (8-10 sentences) covering the following:

> Which stage of the evolution of compliance management (e.g., anti-corruption, institutionalisation, digitalisation) you consider most influential for modern organisations?
> Why is this stage significant?
> How does it shape today's understanding of compliance?
> Which elements of this stage are visible in organisations today?

Target Questions

1. How has the concept of compliance management evolved from its early regula-

tory origins to its modern strategic role in organisations?
2. What are the core principles of compliance management, and why are they essential for building an effective compliance culture?
3. Which key functions does a compliance management system perform, and how do these functions support organisational integrity and risk prevention?
4. What are the main domains of compliance management in contemporary organisations, and how do they interact with broader corporate governance processes?
5. How do international standards (particularly ISO 37301:2021) define the structure and requirements of an effective compliance management system?
6. What are the main features and current challenges of compliance management development in Ukraine compared to international (especially EU) practice?

References for Self-study

1. Airbus. (n.d.). Integrity and compliance. https://www.airbus.com/en/sustainability/integrity-and-compliance
2. Deutsche Telekom. (n.d.). TellMe whistleblower portal. https://www.telekom.com/en/company/compliance/details/tellme-whistleblower-portal-356032
3. Devitt, J. K. (2015). What is Whistleblowing? In: Speaking Up Safely Civil Society Guide to Whistleblowing: Middle East and North Africa Region. Transparency International, Jan.1, 5-7. http://www.jstor.org/stable/resrep20533.4
4. European Union. (2019). *Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law (Whistleblower Protection Directive).* https://eur-lex.europa.eu/eli/dir/2019/1937/oj/eng
5. Gramont, Jacqueline de (2017). The Business Case for "Speaking Up". How Internal Reporting Mechanisms Styrengthen Private-Sector Organisations. Transparency International. 16 p. https://www.transparency.org/en/publications/business-case-for-speaking-up
6. Jones, A. (2015). The role of employee whistleblowing and raising concerns in an organizational learning culture – elusive and laudable? *International Journal of Health Policy and Management, 5*(1), 67–69. https://doi.org/10.15171/ijhpm.2015.182
7. Labour Code of Ukraine (No. 322-VIII, December 10, 1971). https://zakon.rada.gov.ua/laws/show/322-08
8. Law of Ukraine On Civil Service (No. 889-VIII, December 10, 2015). https://zakon.rada.gov.ua/laws/show/889-19
9. Law of Ukraine On Electronic Identification and Electronic Trust Services (No. 2155-VIII, October 5, 2017). https://zakon.rada.gov.ua/laws/show/2155-19
10. Naftogaz Group. (n.d.). *Naftogaz launches the Trust Line in a new format.* https://www.naftogaz.com/news/trust-line-new-format
11. National Agency on Corruption Prevention (NAZK). (2023, September 6). *Launch of the unified whistleblowing portal.* https://nazk.gov.ua/uk/novyny/6-veresnya-

nazk-zapuskaye-yedynyj-portal-povidomlen-vykryvachiv

12. NAVEX Global. (2025). Whistleblowing and incident management benchmark report. NAVEX Global. https://cdn.navex.com/image/upload/v1742410133/resources-2025/benchmarking-reports/2025-navex-whistleblowing-incident-mgt-benchmark-report.pdf
13. Nowers, I. & Terracol, M. (2025). Monitoring Internal Whistleblowing Systems. A framework for collecting data and reporting on performance and impact. Transparency International and Transparency International Ireland. 44 p. https://www.transparency.org/en/publications/monitoring-internal-whistleblowing-systems
14. Order of the Cabinet of Ministers of Ukraine No. 1351-r of December 31, 2024 On the Strategy for Digital Development of Innovative Activity of Ukraine until 2030. https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80
15. Order of the National Agency on Corruption Prevention (NACP) No. 127/20 of April 2, 2020 On Approval of the Requirements for the Protection of Anonymous Communication Channels for Reporting Possible Facts of Corruption or Corruption-Related Offences. https://zakon.rada.gov.ua/laws/show/z0370-20
16. Organisation for Economic Co-operation and Development. (2016). *Committing to effective whistleblower protection.* OECD Publishing. https://doi.org/10.1787/9789264252639-en
17. Paine, L. S. (1994). Managing for organizational integrity. *Harvard Business Review, 72*(2), 106–117. https://hbr.org/1994/03/managing-for-organizational-integrity
18. Park, H., & Blenkinsopp, J. (2009). Whistleblowing as planned behavior: A survey of South Korean police officers. *Journal of Business Ethics, 85*, 545–556. https://doi.org/10.1007/s10551-008-9788-y
19. Rashid, I. (2025). ISO 37301:2021 Compliance Management Systems – An Overview. LinkedIn. https://www.linkedin.com/pulse/iso-373012021-compliance-management-systems-overview-irfan-rashid-auvif
20. Siemens Energy. (n.d.). *Reporting channels "Speak Up" and Ombudsperson.* https://www.siemens-energy.com/global/en/home/company/compliance/reporting-channels.html
21. Shalimova N., Fomenko A. (2024). *Compliance management system in Ukrainian higher education institutions: implementing and transforming.* In Martina Rašticová, Nataliia Versal, Nataliia Tkalenko, (Ed.), Resilient and Sustainable Future: ESG in Higher Education: monograph. Riga, Latvia : Baltija Publishing, pp. 198-215. URL: https://doi.org/10.30525/978-9934-26-507-5
22. Terracol, M. (2024), *Internal Whistleblowing Systems – Self-Assessment Framework for public and private organisations.* https://www.transparency.org/en/publications/internal-whistleblowing-systems-self-assessment-framework-public-private-organisations
23. Terracol, Marie (2022). Internal whistleblowing systems. Best practice principles

for public and private organisations. Transparency International. 46 p. https://files.transparencycdn.org/images/2022_PolicyBrief_InternalWhistleblowingSystems_English-1.pdf

Assignments for Self-Study

1. Analyze 2-3 articles or cases about corporate scandals and explain how the lack of compliance control influenced their occurrence.
2. Review the key principles of compliance management mentioned in the chapter (good governance, transparency, proportionality, accountability, integrity).
3. Prepare a short table with: the principle; its meaning in simple words; a practical example of how it could be applied in an organisation
4. Examine the main domains of compliance management
5. Based on the “Main Domains of Compliance Management” section, choose two domains and for each domain briefly describe: its purpose; typical risks; basic compliance measures used in practice.
6. Create a simple conceptual map (mind map) that shows the relationships between the following elements: compliance; compliance obligations; compliance culture; compliance management system; integrity.

Learning Outcomes

After studying this chapter, learners will be able to:

- Understand the theoretical foundations of business ethics, integrity, compliance, and corporate culture in modern organisations.
- Identify key ethical risks, behavioural factors of misconduct, and fraud prevention mechanisms in the corporate environment.
- Understand the structure and practical elements of an effective ethics and compliance programme, including leadership, values, controls, and organisational procedures.

Key words: Business Ethics, Integrity, Compliance, Corporate Culture, Code of Conduct, Corporate Governance, Whistleblowing.

Main definitions

In the modern business environment, ethics is one of the essential aspects of effective management. The term *business ethics* is defined as a field that studies moral principles and norms aimed at shaping the behaviour of organisations and their employees in the process of making management and economic decisions.

Geddes (2017) emphasises that *business ethics* addresses the permissibility of certain practices and is based on moral principles that reflect perceptions of right and wrong behaviour in the business environment. Unlike compliance, business ethics is not limited to abiding by laws but encompasses a broader range of values, such as honesty, responsibility, and fairness.

According to Weber & Wasieleski (2013), *business ethics* forms the basis of corporate ethics programmes aimed at regulating employee behaviour and reducing the risk of misconduct within the organisation. The authors argue that for business ethics to be effective, it must be integrated into a company's strategy and supported by corporate culture.

Therefore, *business ethics* can be defined as the foundation of a system of norms and values in business that shapes expectations regarding the behaviour of organisations and their interactions with stakeholders.

Integrity is an important part of business ethics, essential for achieving various ethical business goals. Contemporary research emphasises that the concept of integrity is often viewed as a more internal, values-based approach compared to compliance.

According to Geddes (2017), the meaning of *integrity* lies in the consistency between an organisation's stated values, actual behaviour, and decisions. Integrity in business ethics implies honesty and moral consistency that organisations and their employees adhere to even under pressure or adverse circumstances.

Tullberg (2012) defines *integrity* as the stability of values and their practical implementation in actions. The author argues that integrity in an organisation is manifested in its behaviour, consistent with the declarative values of the organisation.

Furthermore, Jacobs (2004) emphasises that *integrity* in the business environment is directly linked to self-regulation and employees' moral judgement. In contrast to compliance, which requires formal adherence to rules, integrity assumes the ability to make ethically sound decisions in situations where clear instructions are lacking.

In general, *integrity* can be characterised as the key element of an ethical culture that forms a person's internal motivation for responsible behaviour.

In academic literature, *compliance* is traditionally characterised as adherence to laws, regulations, and internal company rules. Compliance-focused organisations establish rules and norms of conduct with expected penalties for non-compliance.

According to Geddes (2017), the *compliance culture* in an organisation is formed under the influence of external regulation and is aimed at preventing violations through a well- d system of formal rules, sanctions, and control mechanisms. This approach has become widespread as a result of corporate scandals and the adoption of regulations such as the Federal Sentencing Guidelines.

According to Roberts (2009), *compliance* in an organisation is primarily aimed at minimising legal and financial risks and often motivates employees to act out of fear of punishment rather than based on internal ethical convictions.

(Weber & Wasieleski, 2013) emphasise that effective compliance programmes must go beyond formal compliance with rules and be integrated with the ethical values and culture of the organisation.

Consequently, compliance is a necessary element of business ethics, which provides the legal basis for an organisation's activities, but requires supplementation with value-oriented approaches based on the principles of integrity and ethical culture.

Standards, Laws, and Regulations

1. International: In the context of globalisation, international standards are crucial in shaping unified approaches to business ethics and compliance, as they facilitate the creation of appropriate management systems within organisations focused on legal compliance and strengthening an ethical culture. The key international standard in the field of compliance is ISO 37301, which sets requirements for compliance management systems and emphasises the need to integrate compliance into corporate governance and decision-making processes. This standard is often used as a tool for legal compliance and for developing a culture of integrity and responsibility within an organisation (International Organisation for Standardisation, 2021). In addition to this standard, businesses also actively utilise the UN Global Compact, which provides universal principles in the areas of human rights, labour standards, environmental protection, and anti-corruption, shaping ethical and responsible behaviour within organisations. Together, these international framework initiatives and standards promote the integration of ethical values and integrity into company strategies and practices (United Nations Global Compact, 2023).

2. European Union Regulations: European Union (EU) regulation is an integral part of the uniform requirements for ethical and responsible business conduct within the European Union. Unlike voluntary international initiatives, EU standards are binding and aim to strengthen transparency, accountability and integrity of corporate conduct (European Commission, 2023). One of the significant regulations in the field of business ethics and compliance is the EU Whistleblower Protection Directive (EU Whistleblower Protection Directive 2019/1937). This directive obliges organisations to establish safe channels for reporting violations and to ensure protection for individuals who report misconduct, including violations of law and ethical standards (European Union, 2019). It thereby promotes a culture of openness and accountability within organisations, reducing the risk of concealing unethical or illegal behaviour. Furthermore, current European Union initiatives in the areas of sustainable development and corporate responsibility, including requirements in the areas of Environmental, Social, and Governance and corporate due diligence, emphasise the need to integrate ethical principles and integrity into companies' strategies and decision-making processes (European Commission, 2023). Taken together, the European Union's regulatory framework strengthens the link between compliance and business ethics, creating an institutional foundation for responsible business conduct.

3. National Level: Germany. At the national level, Germany places particular emphasis on integrating business ethics, integrity and compliance principles into its corporate governance system. The German approach is traditionally characterized by a high degree of management responsibility, transparency of management processes, and the development of a sustainable ethical culture in organizations. The central document in the field of business ethics in Germany is the German Corporate Governance Code, which sets out recommendations and principles for the fair and responsible management of companies, emphasising the role of ethical values, integrity and effective compliance systems as elements of good corporate governance and sustainable business development (Government Commission German Corporate Governance Code, 2022). Furthermore, as part of the implementation of European legislation, Germany adopted the Whistleblower Protection Act (Hinweisgeberschutzgesetz), aimed at ensuring safe channels for reporting violations and protecting individuals reporting misconduct. This law strengthens the practical implementation of business ethics principles and promotes a culture of openness and responsibility in organisations (Federal Ministry of Justice, 2023).

Taking these points into account, international standards, European Union regulations, and national legal frameworks form a multi-layered regulatory system aimed at supporting business ethics, integrity, and compliance within organisations. While international initiatives set general ethical guidelines, EU regulations and national legislation ensure their institutionalisation and practical implementation. Together, these mechanisms contribute to the development of an ethical culture and the mitigation of the risks of misconduct in business.

List of Subchapters

2.1. Theoretical and conceptual foundations of ethics and compliance in modern management

2.2. Basic ethical principles and the formation of organizational values

2.3. Behavioural ethics and psychological aspects of misconduct

2.4. Ethical leadership and ethical dilemmas in the corporate environment

2.5. Globalisation of ethical standards and cross-cultural aspects of business ethics

2.6. Mechanisms for preventing and detecting fraud in the ethics and compliance system

2.1 Theoretical and conceptual foundations of ethics and compliance in modern management

Business ethics, integrity, and compliance represent an interdisciplinary field that encompasses corporate governance, organisational behaviour, and regulatory issues. The academic literature examines this topic in terms of the development of an ethical culture, the importance of values in management decision-making, the effectiveness of formal control mechanisms, and the role of leadership and corporate culture in preventing and al misconduct.

A number of researchers pay particular attention to the value-oriented approach to business ethics and the concept of integrity. For example, Geddes (2017) views integrity as the foundation of ethical behaviour in organisations and contrasts the integrity-based approach with formal compliance, emphasising the importance of integrating both elements to create an effective ethical organisational environment. Similarly, Jacobs (2004) and Tullberg (2012) emphasise the role of moral integrity, self-regulation, and consistency between values and behaviour as key elements of a sustainable ethical culture in business. Other researchers focus on the institutional and managerial aspects of compliance and corporate ethics programmes, emphasising their importance in shaping ethical and lawful behaviour in organisations. Roberts (2009) analyses the development of compliance-oriented models of ethics management, pointing out their focus on risk reduction and compliance with regulatory requirements. Weber & Wasieleski (2013) complement this approach by emphasising the need to integrate formal compliance mechanisms with ethical values and corporate culture to achieve long-term effectiveness.

Research in the field of business ethics, integrity, and compliance demonstrates that sustainable and responsible organisational behaviour cannot be achieved solely through formal rules and control mechanisms. The authors emphasise the need to integrate value-based approaches, integrity principles, and compliance tools into a unified corporate governance system, which creates a basis for analysing practical examples and cases of applying business ethics in organisational activities.

Compliance and GRC are often used interchangeably, but they are not identical. *GRC (Governance, Risk, and Compliance) is an integrated management structure that combines corporate governance, risk management, and compliance (adherence to standards).* Compliance, in its most practical sense, answers the question «are we

acting in accordance with requirements?» and focuses on compliance with legislation, regulatory rules, contractual obligations, internal policies and procedures. It works as a mechanism for preventing violations and as a control system that must prove that the organisation is acting lawfully and predictably.

Governance is a broader category and concerns how an organisation is structured as a system of decision-making and control. It answers the questions «who makes decisions, on what basis, how is implementation controlled, and who is responsible?»

Risk management focuses on uncertainty and its impact on the organisation's objectives. Compliance risk is one category of risk, but it does not encompass all others. For example, the risk of production stoppage due to a power failure is an operational risk, and it can be critical, even though there may be no direct violation of the law. At the same time, violating sanctions by paying a counterparty on the sanctions list is a compliance risk that has legal, financial, and reputational consequences. Risk management determines what is critical for the organisation and how to measure it, while compliance ensures compliance with the requirements that regulate the management of such risks.

Integrity and ethics are about «doing the right thing» even when the law or policy does not explicitly prohibit a particular action. Ethics answers the question «is this consistent with our values, is it fair to the customer, partner, society, does it undermine trust?» Compliance usually formalises a minimum standard: what is definitely not allowed and what must be done. Ethics and integrity set a higher standard of behaviour and shape a culture in which people make the right decisions without fear of punishment and without having to wait for instructions in every case. A simple example: a company sells a complex product to a customer. Legally, it can disclose information in small print, and formally this may be «compliant» with the requirements. But an ethical approach would require ensuring that the customer truly understands the risks, that there is no manipulation, and that the product meets the customer's needs. In this case, compliance may say «there must be a form of disclosure,» while ethics may say «you need to explain honestly, even if it reduces sales.»

The GRC approach combines governance, risk, and compliance into a single managed system so that the organisation does not have three «parallel worlds» where management lives its own life, risk management creates separate matrices, and compliance writes policies that no one reads. GRC focuses on integration: ensuring that goals, risks, controls, accountability, reporting, data for monitoring and incident response are linked. For example, if a company exports, it runs the risk of violating sanctions and export controls. In the GRC model governance ensures that there is a committee or responsible officer who approves rules and controls critical decisions; risk management identifies risk scenarios, risk levels and key indicators, such as the proportion of high-risk transactions or the number of screening «false positives»; Compliance ensures sanctions screening of counterparties, verification of ultimate beneficiaries, escalation procedures and documentation. When this is integrated, the sales manager sees not «another barrier» but part of a system that protects the company and enables safe development.

An important difference between compliance and GRC is that compliance can exist as a separate function, while GRC is more of a management approach where functions are aligned. If compliance works in isolation, it often turns into «control for control's sake»: lots of policies, little impact. If GRC is implemented maturely, compliance becomes not a hindrance but part of the management logic: risks are understood, control measures are proportionate, decisions are documented, and the culture supports integrity.

To summarise, compliance is about meeting requirements and monitoring adherence to rules; governance is about the architecture of responsibility and accountability; risk management is about managing uncertainty regarding goals; integrity and ethics are about behaving correctly beyond minimum requirements; GRC is about integrating all of this into a single working system where rules, risks and management do not contradict each other but reinforce each other (Table 2.1).

Table 2.1 Comparison of ethics, compliance, governance and risk management

Concept	Main goal	Main focus	Example
Governance	Effective management of an organisation	Power structure, accountability	creation of a supervisory board
Risk management	Managing uncertainty	Identification and minimisation of risks	assessment of financial risks
Compliance	Compliance with legislation and policies	Rules, procedures, control	Counterparty verification
Ethics	Moral correctness of behaviour	Values and integrity	honest customer information

Ethics and compliance are closely related, but they perform different functions within an organisation and address different issues. Compliance focuses on formal adherence to external and internal requirements: legislation, regulatory rules, sanctions regimes, standards, contractual obligations, company policies and procedures. Its key logic is to define rules, translate them into specific requirements for behaviour and processes, and then ensure control, accountability and the organisation's ability to demonstrate compliance. Ethics works differently: it is about the moral evaluation of decisions and behaviour, about conscience, values, justice, respect for people, avoiding harm and maintaining trust. Ethics answers not only the question «is it allowed», but above all the question «is it right», even if it is not formally prohibited.

Basic standards and codes of ethics, integrity and compliance form the normative and methodological basis for building effective compliance management systems in

organisations. Their significance lies in establishing universal principles of honest, transparent and responsible behaviour that can be applied regardless of industry or national jurisdiction. Such standards define expectations for the behaviour of organisations, their management and employees, and offer practical mechanisms for managing risks, preventing violations of the law, combating corruption and fostering a culture of integrity. In modern compliance management practice, international management system standards, professional codes of ethics and the guiding principles of international organisations play a special role.

One of the most important international standards in the field of compliance management is ISO 37301, which establishes requirements for compliance management systems. This standard defines the principles for creating, implementing, maintaining and continuously improving a compliance system in an organisation. Its key idea is to integrate compliance into all business processes and to foster a culture of responsibility and ethical behaviour at all levels of management. In practical terms, this means that issues of compliance with legislation, internal policies and ethical standards must be taken into account when making management decisions, planning activities, interacting with counterparties and implementing corporate strategy. For example, a company that has implemented a system in accordance with this standard may establish a procedure for vetting counterparties before entering into contracts to ensure that potential partners are not involved in corruption schemes or subject to sanctions.

An important addition to this standard is ISO 37302, which contains practical recommendations for the implementation and operation of a compliance management system. This document explains how an organisation can apply the principles of the standard in practice, how to identify compliance risks, how to develop policies and procedures, and how to monitor and evaluate the effectiveness of the compliance system. In practical terms, this can manifest itself, for example, in the creation of internal channels for reporting violations or regular training for employees on ethical behaviour and anti-corruption requirements.

The international standard ISO 37001, which deals with anti-bribery management systems, plays a significant role in the fight against corruption. This standard establishes requirements for procedures to prevent, detect and respond to corruption offences. It provides for the implementation of an anti-corruption policy, assessment of bribery risks, due diligence of counterparties, staff training and the creation of mechanisms for reporting suspicious activities. A simple example of the practical application of such a standard would be a situation where a company plans to enter into a contract with a new supplier. Before signing the contract, it checks the partner’s reputation, analyses its ownership structure and ensures that it is not involved in corruption scandals or illegal practices.

International corporate responsibility guidelines, in particular the Organisation for Economic Co-operation and Development Guidelines for Multinational Enterprises, play an important role in shaping ethical business standards. These principles set out expectations for responsible corporate behaviour in the areas of human rights, labour relations, the environment, anti-corruption and corporate governance transparency.

They aim to ensure that businesses not only comply with minimum legal requirements, but also take into account the interests of society and the environment. For example, a company that adheres to these principles may require its suppliers to comply with standards for safe working conditions and prohibit the use of child labour, even if such requirements are less strictly regulated in a particular country.

Professional codes of ethics also have a significant impact on the development of ethics and compliance systems. They define standards of conduct for representatives of specific professions or organisations. One example is the Code of Ethics for Professional Accountants developed by the International Federation of Accountants. This code establishes the basic principles of professional ethics, including honesty, objectivity, professional competence, confidentiality and professional conduct. In practice, this means that an accountant or auditor must act independently, avoid conflicts of interest and not disclose confidential information about clients or employers. For example, an accountant does not have the right to change financial data at the request of management if this leads to a distortion of financial reporting.

In the field of corporate governance, the principles of ethical leadership and integrity, which are often enshrined in internal corporate codes of conduct, are also important. Such codes establish rules for interaction between employees, with clients, partners and government agencies. They may include provisions on conflicts of interest, gifts and hospitality, protection of confidential information, non-discrimination and responsible use of company resources. For example, a corporate code may require an employee to report any potential conflict of interest to management, such as if a relative works for a supplier company.

International anti-corruption initiatives and corporate responsibility principles, such as the United Nations Global Compact, also play an important role in the development of ethical standards. This initiative calls on companies to adhere to principles in the areas of human rights, labour standards, environmental protection and anti-corruption. Companies that join this initiative voluntarily commit to implementing ethical practices in their activities and regularly reporting on the results.

Thus, international standards and codes of ethics create a comprehensive system of principles and practices aimed at ensuring fair, transparent and responsible operations of organisations. They help companies build effective compliance management systems, foster a culture of integrity and minimise the risks of legal and reputational violations. The use of such standards helps to increase trust on the part of investors, partners, customers and society as a whole, and also ensures stable and sustainable business development in today's global environment.

The conceptual difference is already evident in the source of the norms. For compliance, the source is written and verifiable requirements: laws, regulations, policies, codes, procedures, and standards. For ethics, the source is values and moral principles, which may be partially recorded in a code of ethics, but in real situations often go beyond the scope of any document. A simple example: company law and policy may allow a small gift to be accepted from a partner. Compliance will check whether the limit

has been exceeded, whether an entry has been made in the gift register, and whether there is a direct prohibition in a specific situation. Ethics will ask other questions: will it look like an attempt to influence right now, will it create a sense of «obligation,» will it be comfortable if colleagues or clients find out about it? In other words, compliance records the minimum acceptable, while ethics assesses appropriateness and fairness in context.

Another difference lies in the nature of measurability. Compliance, by its very nature, strives for formalisation: its results can be verified by audits, recorded in reports, and measured by indicators. For example, how many employees have been trained, how many contractors have been checked, how many incidents have been investigated and in what time frame, how many transactions have been stopped due to sanctions screening. Ethics is much more difficult to measure because it involves the quality of judgement, motives, culture, and the ability of people to act with integrity without external coercion. In a simple example, you can «mark» 100% completion of ethics training, but this does not guarantee ethical behaviour if the company actually encourages results at any cost or if management demonstrates double standards.

How ethics and compliance deal with «grey areas» is also important. Compliance works best where there are clear rules and it is possible to say unequivocally what is allowed and what is prohibited. Ethics is particularly necessary where the rules do not provide a direct answer or where formal compliance can cover up manipulation. For example, marketing may prepare an advertisement that does not formally contain false statements but creates a false impression in the consumer's mind through the presentation of information. Compliance may say that there are no legal violations or that they are difficult to prove. An ethical approach will require honest communication and respect for the customer's right to understandable information. In such a situation, ethics raises the bar of behaviour above the legal minimum.

Another conceptual difference lies in motivation. Compliance often relies on external incentives and sanctions: the risk of fines, bans, liability, and reputational damage. Ethics relies on internal motivation: the desire to do the right thing, not to cause harm, to maintain trust and self-respect. A simple example: an employee may refuse to participate in a questionable scheme not because they fear punishment, but because they consider it unfair to customers or society. If a company's ethics are weak and compliance is perceived only as «obstacle avoidance,» people may look for formal loopholes to stay «within the rules» but actually do dishonest things.

Ethics and compliance also differ in terms of their scope of consequences. Compliance often thinks in terms of specific violations and immediate legal consequences. Ethics thinks in terms of trust and long-term reputation, impact on stakeholders, and internal culture. For example, a company can legally comply with personal data requirements by including «consent» in a long form that no one reads. Compliance may consider the task complete once the documents are in order. An ethical approach will require clear language, real choice, minimisation of data collection, and respect for privacy as a value, not just a requirement. This reduces the risk of complaints and conflicts in the future, even if everything is formally «legal» today.

In practice, ethics and compliance can come into conflict if an organisation reduces compliance to a series of «checkboxes». A classic example is a «gift within the limit.» If a manager constantly gives souvenirs to the same official, each of which individually does not exceed the limit, the compliance logic of «everything is allowed individually» may only look convincing on paper. Ethical logic will take into account the cumulative effect, intent and perception, as well as the risk that it will look like systematic influence. That is why mature organisations combine compliance rules with an ethical test of «how it looks from the outside» and a risk-oriented assessment of the context.

At the same time, ethics and compliance are not alternatives; they complement each other. Compliance without ethics becomes formal and prone to «circumvention of rules,» while ethics without compliance becomes a good declaration without tools for implementation and evidence. In a simple example, a company proclaims the value of «honesty,» but if there is no conflict of interest policy, declaration procedures, procurement control, and a mechanism for reporting violations, honesty will not become a practice. On the other hand, if there are dozens of procedures and control forms, but managers demonstrate double standards, employees will quickly realise that «the rules are for others» and compliance will become a facade.

In the learning outcome, conceptual differences can be felt through a simple «question check.» Compliance asks questions about conformity: is there a rule, is it being followed, is there documentary evidence, has approval been obtained, have limits been met, has control been set up? Ethics asks questions about integrity: is it fair, are we misleading anyone, are we creating hidden pressure, are we damaging trust, would we be prepared to explain this decision publicly? For example, if an employee is unsure whether to accept an «informal thank you» from a customer, compliance will respond with a prohibition and a reporting procedure, while ethics will support an internal understanding of why this is unacceptable, even when the chance of exposure seems small. It is precisely this difference between «can/cannot» and «right/wrong» and the ability to act correctly in grey areas that constitutes the main conceptual boundary between ethics and compliance.

2.2. Basic ethical principles and the formation of organisational values

In the modern system of organisational management, the relationship between values, rules and laws plays an important role, as these elements form the basis of employee behaviour, define the limits of acceptable actions and ensure that the organisation’s activities are consistent with the requirements of society and the state. Values, rules and laws can be viewed as different levels of behaviour regulation, which differ in their degree of formalisation, source of origin and method of enforcement (Figure 2.1). In this system, values constitute the deepest level, rules serve as an organisational mechanism for specifying these values, and laws form an external regulatory framework that is binding on all economic entities.

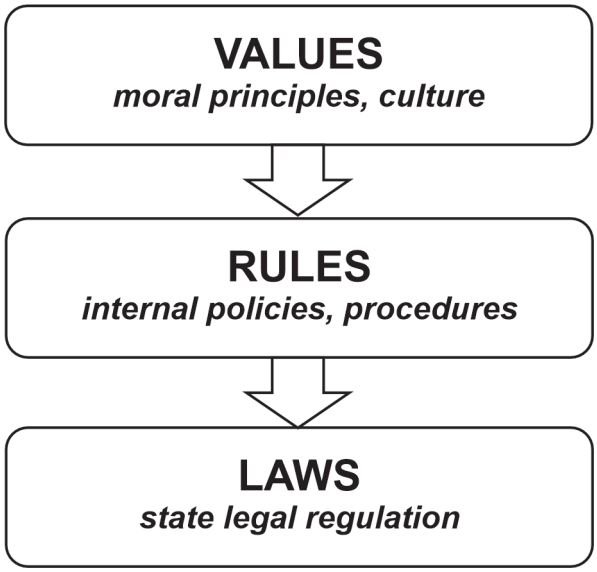


Figure 2.1 Interrelationship between values, rules and laws

Values reflect fundamental beliefs and principles that determine what is considered right, fair and desirable in the behaviour of individuals and organisations. They are shaped by culture, social environment, professional ethics and the strategic priorities of the organisation. In a corporate environment, values are often enshrined in codes of ethics, corporate principles or the company's mission statement. For example, a company may proclaim values such as honesty, responsibility, transparency, respect for customers, or sustainable development. If honesty is a value of the organisation, it means that employees must act truthfully even in situations where there is no direct prohibition or control. A simple example can be seen in a situation where an employee notices an error in an invoice that accidentally brought the company additional profit. The law may not require immediate correction of such an error, but the value of honesty encourages the employee to inform the customer and correct the inaccuracy.

Rules are the next level of regulation and represent formalised behavioural requirements developed by an organisation to implement its values and ensure compliance with legislation. They define specific procedures, restrictions and standards of conduct for employees in various situations. Unlike values, which are more abstract in nature, rules are clearly formulated and can be verified through internal control or audit. For example, if an organisation's values are transparency and integrity, the rule may require mandatory registration of gifts and entertainment expenses. In this case, an employee who receives a souvenir or invitation to an event from a partner must enter the information in a special register and notify their manager or compliance officer. Thus, the rule transforms a general ethical requirement into a specific management procedure.

Laws are the highest level of regulatory control established by the state and are

binding on all individuals and legal entities. They define the legal framework for economic activity, establish liability for violations, and ensure the protection of public interests. In the field of compliance management, laws may regulate issues such as combating corruption, countering money laundering, protecting personal data, competition policy or financial reporting. For example, legislation may expressly prohibit the provision of undue benefits to a public official. In this case, the company must not only comply with this rule, but also establish internal control procedures to prevent such violations. If an employee offers money to an official to expedite the issuance of a permit, this is no longer simply a violation of internal rules or ethical principles, but an offence that may lead to criminal liability.

The relationship between values, rules and laws can be imagined as a kind of system in which each element performs its own function. Values determine the general direction of behaviour and shape corporate culture. Rules detail these principles and make them applicable in the daily activities of the organisation. Laws create a mandatory external framework that protects public interests and sets minimum standards of behaviour. If a company is guided solely by laws, its behaviour is limited to meeting minimum requirements. If, on the other hand, an organisation is guided by its own values and ethical principles, it can act more responsibly and build trust among partners, customers and society.

Values can also be divided into different types depending on their content and role in the behaviour of people and organisations (Table 2.2). Some values are related to moral principles and define ideas about good and evil, justice and responsibility. Others relate to professional activities and shape standards of quality, efficiency or innovation. Social values, which reflect attitudes towards society, the environment and sustainable development, constitute a separate group. For example, the moral value of honesty is manifested in truthful reporting and the absence of manipulation of financial data. The professional value of quality can mean the desire of employees to perform their work as accurately and responsibly as possible. The social value of environmental responsibility can be manifested in the introduction of environmentally friendly technologies or the reduction of emissions in production.

Table 2.2 Types of organisational values

Type of values	Characteristic	Example of manifestation
Moral	define the concepts of good and justice	honesty in reporting
Professional	define work standards	quality and competence
Social	reflect responsibility to society	Environmental policy
Corporate	shape the culture of the organisation	openness of communication

There are also individual and corporate values. Individual values are formed at the personal level and depend on a person's upbringing, education and life experience. Corporate values are formed by the organisation's management and enshrined in internal documents, but they only become real when they are supported by the behaviour of employees and managers. For example, a company may proclaim the value of openness, but if management does not allow criticism or does not respond to reports of violations, this value will remain declarative.

In the context of compliance management, it is important that values, rules and laws do not contradict each other, but form a single logical system. If laws establish minimum requirements, the organisation's rules must specify how they are to be implemented, and values must shape a culture of behaviour in which compliance with these requirements becomes a natural part of the business. For example, the law may require the fight against corruption, internal rules may define procedures for checking counterparties and maintaining a register of gifts, and the value of integrity shapes employees' attitudes towards these procedures not as a formality, but as an important element of the organisation's responsible activities.

Thus, values, rules and laws are interrelated elements of a system for regulating behaviour within an organisation. Values form the moral foundation and corporate culture, rules ensure the practical implementation of these principles in everyday activities, and laws establish mandatory legal boundaries for the organisation's functioning in society. Their consistency and complementarity create the conditions for the formation of an effective compliance management system based on integrity, responsibility and respect for legal and ethical standards.

Basic ethical principles and organisational values constitute an internal «compass» for the behaviour of the organisation and its employees, which determines not only what is formally permitted or prohibited, but also what is considered correct, fair and acceptable in professional interactions. Ethical principles are essentially general norms that set the direction for moral judgement and choice, while organisational values are the established priorities and beliefs of a particular company that shape its culture, management style, approaches to customers and partners, and criteria for evaluating staff behaviour. In compliance management practice, ethical principles and values interact in such a way that principles answer the question «how to act,» while values explain «why» and «what our organisation should be like.»

One of the basic ethical principles is honesty, which means truthfulness, absence of deception and manipulation, as well as a willingness to call things by their proper names even when it is inconvenient or temporarily disadvantageous. In a simple example, honesty is demonstrated when a sales manager does not promise a customer a delivery date that is known to be impossible to meet, even if it would help to close the deal. At the organisational level, honesty as a value is supported by transparent communications, accurate advertising, realistic commitments and

the absence of the practice of «embellishing» performance indicators in reports. When a company talks about honesty as a value, it is effectively committing not to shift risks onto the customer covertly and not to create illusions for partners or investors.

Fairness as an ethical principle concerns the equality of rules, impartiality, and proportionality of decisions. It manifests itself in the fact that similar situations should be treated in a similar manner, and differences in decisions should have reasonable causes rather than depend on personal sympathies or status. A simple example of fairness is when a company applies the same rules for business trips or bonuses to both managers and ordinary employees, and exceptions are explained by objective needs rather than «because that's the way it's always been done.» Fairness as an organisational value is also reflected in transparent supplier selection procedures, where decisions are based on criteria of quality, price and risk, rather than informal agreements or «our people».

Respect for human dignity is a principle that determines the style of interaction within the team and the attitude towards customers and partners. It is not just about politeness, but about recognising the right of others to safe working conditions, non-discrimination, privacy and fair treatment. In a simple example, respect is shown when a manager does not use humiliation as a «method of motivation,» does not tolerate toxic jokes, and creates conditions where an employee can express their professional position without fear of retaliation. At the customer level, respect means that the company does not use dark patterns in digital services, does not force users to accidentally agree to unnecessary services, and does not abuse information asymmetry.

Responsibility as an ethical principle implies a willingness to acknowledge the consequences of one's decisions, keep promises, and correct mistakes. In practice, this means not looking for someone to blame «for the sake of it,» but understanding the causes and building a system that prevents recurrence. A simple example of responsibility is when a company discovers an error in an invoice and does not wait for the customer to complain, but initiates a correction itself, explains the situation, and apologises. Responsibility as an organisational value is also important in the context of ESG: if a company declares environmental responsibility, it strives not just to «do the minimum,» but to actually reduce its impact on the environment, invest in safe technologies, and report transparently on its results.

The principle of transparency is closely related to honesty, but has a separate emphasis: it is about the openness of essential information, the absence of hidden conditions and the clarity of decisions. In a simple example, transparency means that the terms of the contract are written clearly, penalties are not hidden in small print, and key risks are explained to the customer. In an organisational context, transparency manifests itself in clear approval procedures, clear rules on conflicts of interest, the existence of gift registers, and the ability to track who made a decision and on what basis. It is transparency that makes ethical

standards practically verifiable, as it reduces the «grey areas» where abuse can occur.

Integrity as a principle is integrative: it means consistency between words and actions, the absence of double standards, and internal integrity. Integrity is very noticeable in small details. A simple example: if a company declares zero tolerance for corruption but turns a blind eye to the questionable practices of a key salesperson who brings in high revenues, then the value becomes a fiction and the culture becomes cynical. Conversely, if even a «star» employee faces consequences for violations, the team gets the message that the rules and values are real. Integrity as an organisational value is often reflected in how a company responds to incidents: whether it tries to hide the problem or acknowledges it, investigates it, corrects it and learns from it.

Legality as an ethical principle in a corporate context means respect for the law and a willingness to act within the norms not only formally but also in substance. It is important to understand that legality is not limited to «circumventing the rules.» A simple example: a company may look for a scheme to formally comply with procurement requirements, but in fact ensure the victory of the «right» supplier. Formally, it is possible to create the appearance of a procedure, but the ethical principle of legality requires ensuring real competition, equal conditions and the absence of bias. When legality becomes an organisational value, a company builds compliance not as a defence against penalties, but as the basis for trust in the business.

Loyalty and care for the organisation as a value also have an ethical dimension, but they must be balanced with integrity. Loyalty does not mean covering up violations; in a mature culture, loyalty means a desire to protect the company from harm, including by reporting problems. A simple example is when an employee notices that a colleague is bypassing counterparty verification procedures and understands that this could lead to sanctions violations. Ethical loyalty does not mean « « covering for a colleague, but rather reporting correctly through an internal channel so that the company can eliminate the risk.

Organisational values usually manifest themselves as stable guidelines that influence everyday decisions. The value of customer focus in an ethical sense does not mean «sell at any cost,» but rather ensure customer benefit, fair terms, and no coercion. The value of professionalism means competence, evidence-based decisions, and a willingness to improve qualifications. The value of cooperation means mutual support and honest communication between departments, where risks are not hidden due to competition for budgets or KPIs. Innovation as a value in an ethical context means that new technologies are implemented with safety, privacy and human impact in mind, not just for speed and profit.

To ensure that ethical principles and values do not remain mere declarations, they must be «embedded» in daily processes (Figure 2.2).

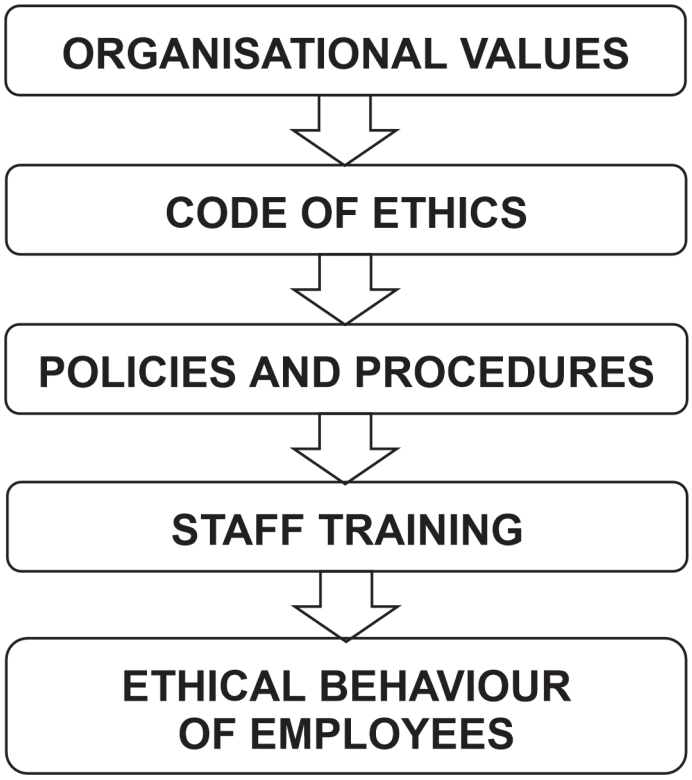


Figure 2.2 Mechanism for shaping ethical behaviour in an organisation

This manifests itself when hiring, not only skills are assessed, but also the willingness to act with integrity; when the incentive system does not reward violations «for results»; when managers set an example and do not take advantage of exceptions; and when employees have a safe way to ask questions or report problems. A simple example of such integration is when, before signing a contract with a new partner, an employee does not perceive due diligence as «excessive bureaucracy» but as a manifestation of responsibility and transparency, because the organisational value of integrity makes it a natural part of the job.

As a result, ethical principles set universal criteria for morally correct decisions, and organisational values transform these criteria into the character of the company, its culture and standards of interaction. When they are aligned, it is easier for employees to act correctly even in complex «grey» situations where there are no direct instructions, and the organisation gains stability, trust and better quality management decisions.

2.3. Behavioural ethics and psychological aspects of misconduct

Behavioural ethics views ethical decisions not as an abstract choice between «good and evil,» but as the result of real human psychology, limited attention, emotions, social pressure, habits, interests, and organisational environment characteristics (Table 2.3). Its key idea is that most wrongful or unethical actions in companies are not committed

by «cartoon villains» but by ordinary people who perceive themselves as decent but gradually find themselves in situations where violations seem acceptable, justified or even «necessary.» The psychology of misconduct explains how this shift in boundaries occurs, why people do not notice their own unethical behaviour, how self-deception and rationalisation work, and why organisational incentives are sometimes stronger than internal moral guidelines.

Table 2.3 Key psychological factors of misconduct

Psychological factor	Essence	Example
Rationalisation	justification of violations	“everyone does it”
Social pressure	influence of management or team	requirement to fulfil the plan
Conflict of interest	Personal gain influences decisions	Choice of a familiar supplier
Gradual shift in norms	minor violations become commonplace	Adjustment of reporting

One of the most common reasons for misconduct is that people tend to «relax their ethics» in everyday decisions (Figure 3.3).

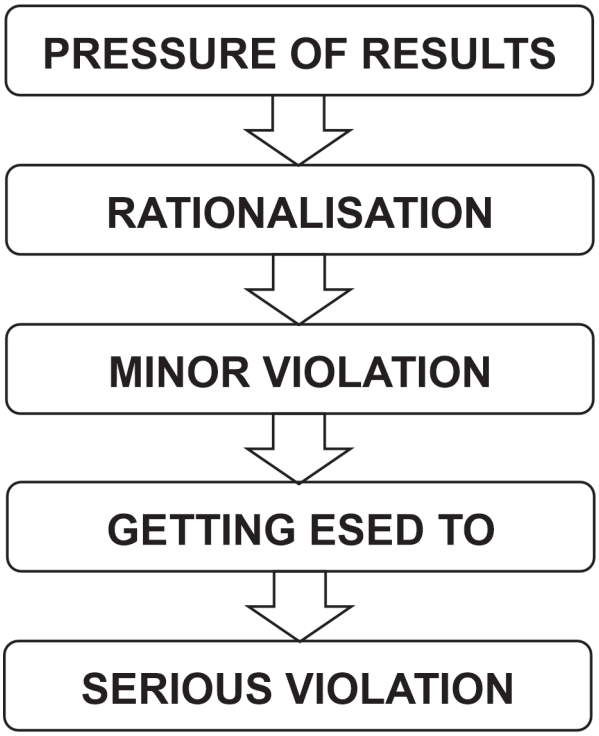


Figure 2.3 Psychological mechanism of the emergence of disorders

When the choice seems minor, people do not engage in moral evaluation and perceive the situation as purely work-related. A simple example can be seen in procurement: a manager chooses a «familiar» supplier because it is faster and does not conduct a full check of documents, even though the procedure requires it. In his mind, this does not look like a violation, but rather like time optimisation. But it is precisely such «minor» deviations that over time create a culture where rules are considered conditional, and in this culture it is much easier to move on to serious violations, such as kickback agreements or tender manipulation. An important mechanism is moral rationalisation, when a person finds an explanation that allows them to maintain a positive image of themselves, even if the action is wrong. A person may convince themselves that «everyone does it,» that «it's temporary,» that «the company is rich and won't suffer,» that «I'm doing it for the team,» or that «it's not a bribe, but a thank you.» In a simple example, a salesperson may promise a customer a product feature that does not yet exist and justify it by saying that «it will be added anyway» or that «otherwise the deal will go to a competitor.» Psychologically, they absolve themselves of responsibility for deception by turning it into a «prediction» or «marketing ploy.» Such rationalisations are dangerous because they do not feel like lies and therefore do not trigger an internal «stop signal».

An important mechanism is moral rationalisation, when a person finds an explanation that allows them to maintain a positive image of themselves, even if the action is wrong. A person may convince themselves that «everyone does it,» that «it's temporary,» that «the company is rich and won't suffer,» that «I'm doing it for the team,» or that «it's not a bribe, but a thank you.» In a simple example, a salesperson may promise a customer a product feature that does not yet exist and justify it by saying that «it will be added anyway» or that «otherwise the deal will go to a competitor.» Psychologically, they absolve themselves of responsibility for deception by turning it into a «prediction» or «marketing ploy.» Such rationalisations are dangerous because they do not feel like lies and therefore do not trigger an internal «stop signal».

Another powerful factor is the gradual shift in norms, sometimes referred to as the «slippery slope effect.» It is rare for a person to commit a major crime right away. More often, they make a small deviation, then another, then it becomes a habit, and the line of what is acceptable moves.

Social influence and submission to authority often explain people's behaviour even better than «greed». People are guided by what others do, especially if those others have status, experience or power. If a manager signals that results are more important than rules, subordinates may feel that following procedures is a weakness. A simple example: a manager says, «I don't care how you do it, just get the job done.» Formally, this is not an order to break the law, but for the employee, it is psychological permission to circumvent the rules. In such conditions, an employee may agree to risky deals, «turn a blind eye» to sanctions restrictions, or sign documents without checking them because they are afraid of losing their job, bonus, or the respect of their manager.

Conflict of interest is a special type of situation where psychology works very insidiously. A person may sincerely believe that their decisions are objective, but their own benefit imperceptibly changes their perception of facts and risks. A simple example: a manager

recommends a supplier with whom they have a friendly relationship and convinces themselves that this is «the best option,» even though they have not analysed the alternatives as thoroughly. He may not perceive this as corruption because he did not receive any money. But psychologically, he is no longer neutral, and the organisation is at risk of inflated prices, low quality and reputational damage.

An important topic in behavioural ethics is moral «disengagement,» when a person temporarily stops perceiving others as people with rights and dignity and sees only obstacles or means. This can manifest itself in sales, marketing, debt collection, and work with vulnerable groups. A simple example: a company may use manipulative messages to force a customer to subscribe to a service and justify it by saying, «It's just business.» At this point, the customer ceases to be a person to be respected and becomes a «conversion.» This shift in perception makes unethical practices «normal» and creates risks of complaints, sanctions, and loss of trust.

An additional mechanism is diffusion of responsibility, when in complex organisations people feel that «it's not my job», «I'm just an executor» or «another department is responsible for that». The more links there are in the process, the easier it is to hide behind the system. A simple example: a compliance officer notices a suspicious transaction but thinks that «financial monitoring will sort it out»; financial monitoring thinks that «lawyers will assess it»; lawyers think that «the business should provide an explanation»; and the business puts it off because «there is no time.» As a result, the risk is realised not because of malicious intent, but because of a psychological dilution of responsibility.

Incentives and metrics have a strong influence. When the system rewards only financial results or speed, and ethical behaviour is irrelevant to the assessment, people tend to «optimise» precisely what is measured. A simple example: if a manager's bonus depends only on the number of contracts signed, they will be inclined to skip counterparty checks or hide risks because they slow down deals. If the evaluation system includes quality, compliance with procedures, and the absence of incidents, behaviour changes because the psychological focus of attention changes.

Behavioural ethics emphasises that people often do not realise the moral dimension of a situation at the moment of decision-making. In the fast pace of work, a person sees the task as operational: «we need to ship urgently,» «we need to close the month,» «we need to sign the contract.» Moral judgement comes later, when the consequences become apparent. A simple example: an employee agrees to «sign retroactively» because «it's more convenient for everyone,» without thinking that this could be document falsification. It seems to them to be an administrative formality, although in fact it creates legal risks.

From a compliance and ethics management perspective, it is important to understand that misconduct is often a predictable response to the environment. If fear, silence about problems, and punishment for bad news are the norm in an organisation, people will hide incidents and «paint» indicators. If it is customary in an organisation to discuss difficult cases, if reporting a problem is not punished, if managers demonstrate consistency, then psychological mechanisms work in favour of integrity. A simple example of a

healthy environment: an employee is unsure whether to accept an invitation to an event from a supplier and, without fear, turns to compliance; the risks are explained to him, he chooses the safe option, and the decision is recorded. In a toxic environment, the same employee may remain silent because he does not want to appear «difficult,» and the risk increases.

Thus, behavioural ethics and the psychology of misconduct explain that violations often arise not because of a lack of rules, but because of human cognitive distortions, social pressure, conflicts of interest, misguided incentives, and organisational culture. Understanding these mechanisms helps to build a compliance system not only as a set of prohibitions, but as an environment in which correct behaviour becomes easier, more natural and supported by both formal procedures and a living culture of integrity.

2.4. Ethical leadership and ethical dilemmas in the corporate environment

Ethical leadership is a management style in which the manager does not simply demand compliance with the rules, but demonstrates morally responsible behaviour on a daily basis, fosters a culture of fairness and trust, and creates conditions in which it is easier for employees to do the right thing than to look for «loopholes». It is a combination of personal example, consistency of decisions, transparency of motives, and the manager's ability to balance the interests of the organisation, customers, employees, and society. In compliance management practice, ethical leadership is critically important because it is managers who set the real «rules of the game»: if they informally encourage results at any cost, even the best policies will perform poorly; if managers consistently uphold integrity, then rules and standards become alive, rather than declarative.

An ethical leader is distinguished by the fact that they think not only in terms of what is allowed or prohibited, but also in terms of trust, fairness, responsibility and long-term consequences. For example, in procurement, a manager may not formally violate procedures, but may unethically pressure the commission to «correctly» evaluate the proposal of the desired supplier. Ethical leadership means the opposite: a manager ensures fair competition, allows uncomfortable questions, supports independent control, and is ready to make a decision that is temporarily less profitable but reduces the risk of corruption and reputational damage. A simple example of ethical leadership in daily work looks like this: a sales manager brings in a deal that generates a large profit, but the counterparty shows signs of high risk and the documents are incomplete. An unethical manager will say, «Close it quickly,» while an ethical manager will stop the process, demand proper verification, and explain to the team that reputation and legality are more important than short-term results.

Decision-making models in the context of ethical leadership are not needed to «make morality bureaucratic,» but to give employees a clear logic for action in complex situations where there are conflicts of interest, time pressure, ambiguous norms, or «grey areas» (Table 2.4). Ethical decisions often require an assessment of context,

intentions, and consequences, as well as a check to see whether fear, gain, or group expectations are distorting the choice (Figure 2.4). That is why leaders who practise ethical leadership typically teach their teams to think through simple, understandable decision-making «filters» and foster an atmosphere where ethical issues can be discussed openly.

Table 2.4 Ethical decision-making models

Model	Essence of the approach	Example
Legal model	Verification of compliance with laws	Does the decision violate the law?
Ethical model	Compliance with values	is it fair to the client
Consequence model	assessment of impact on stakeholders	will reputation be damaged
Publicity model	Openness test	Will it be embarrassing to make the decision public?

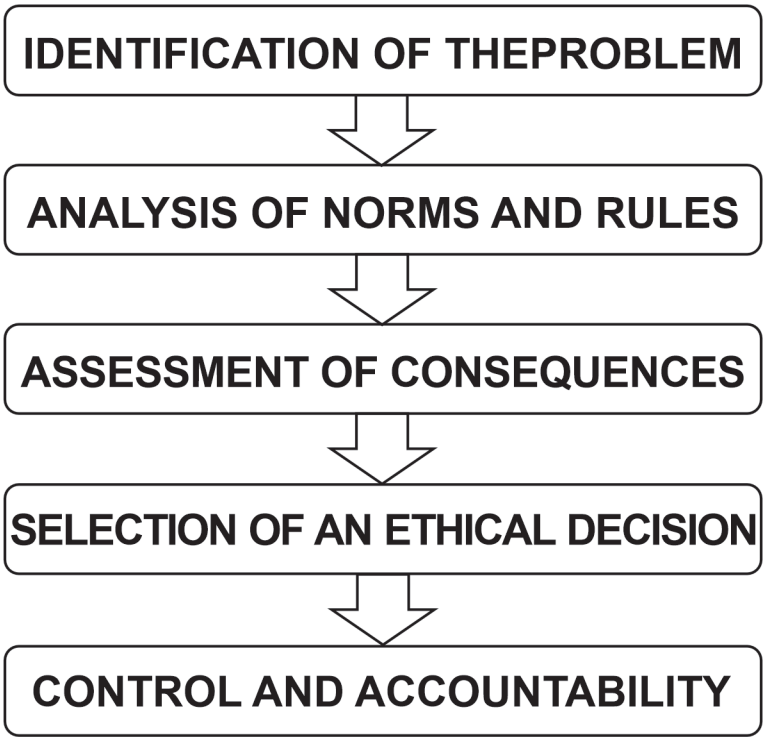


Figure 2.4 The process of ethical management decision-making

One of the most practical approaches to ethical decision-making can be described as a model of compliance and integrity, where decisions go through two levels of verification. At the first level, the action is assessed for compliance with the law, company policies and compliance requirements. At the second level, it is assessed whether the action is consistent with values, whether it is fair, whether it is misleading, and whether it maintains trust. A simple example: an employee is offered a gift from a partner within the permitted amount. At the compliance level, the answer may be «yes, if registered.» At the value level, the question arises as to whether it is appropriate at this particular moment, for example during contract negotiations, and whether it will appear to be influence peddling. The ethics manager will advise the team that even if it is formally possible, we must assess the context so as not to create the risk of bias.

A common practice is the impact assessment model, where a decision is analysed from the perspective of who benefits and who may be harmed. This approach works well when there is a risk of «convenient self-deception» that there is no harm. A simple example: marketing prepares an advertising message that is not formally untrue, but may mislead the customer about the real cost of the service. An ethical manager will ask the team to look at the consequences through the eyes of the customer: will they understand the real conditions, will they feel cheated, will this lead to mass complaints and loss of trust? Even if the ad boosts sales in the short term, it could ruin the brand's reputation in the long run, and ethical leadership is what stops that kind of decision.

Another useful approach is related to the principle of fairness and equality of rules, where the manager checks whether the decision applies equally to different people and whether it creates double standards. A simple example: a company punishes an ordinary employee for violating a procedure, but «turns a blind eye» to a similar violation by a manager because he brings great results. This destroys the ethical climate: people begin to consider the rules to be fiction and learn to circumvent the system. An ethical leader acts differently: they show that the standards are the same for everyone and that it is the position that obliges them to be an example, not that it grants immunity.

In management practice, the so-called «publicity test» is often used, when a manager asks a simple question: would we be comfortable if this decision became known to colleagues, customers, auditors, journalists or regulators? This test does not mean that everything has to be public, but it helps to identify situations where decisions are based solely on secrecy. A simple example: a manager wants to «negotiate» with an inspector to avoid unnecessary inspections. If even the thought of publicity causes fear and shame, it is a strong signal that the action is wrong. Ethical leadership is about teaching the team to use such a simple moral test and not to dismiss it as «naivety.»

An important part of ethical leadership is managing conflicts of interest, as this is where grey areas most often arise. An ethical leader not only requires the disclosure of conflicts of interest, but also creates a culture where this is not perceived as suspicious, but as normal practice of transparency. A simple example: a project manager has a relative in a supplier company. The ethical decision is not to «say nothing, because we are honest,» but to openly declare the connection and transfer the final choice of supplier to another person or commission. This simultaneously protects the manager from suspicion and the company from corruption risks.

Ethical leadership is also closely linked to the ability to make decisions under pressure and uncertainty. Many violations occur when time is short, the plan is on fire, and the manager sends the signal to «find a way out.» An ethical manager recognises the reality of pressure but does not allow it to become an excuse for violation. A simple example: before the end of the quarter, the head of the finance department receives a proposal to «tweak the numbers a little» to show better results. An ethical manager stops this, explains to the team that investor confidence and legality are more important, and looks for legal ways to improve performance in the future, for example through process optimisation or planning review, rather than through manipulation.

It is worth emphasising that ethical leadership is manifested in how a manager responds to mistakes and reports of violations. If employees see that «bad news» is punished, they will begin to hide problems, and risks will accumulate. An ethical manager acts in such a way that people are not afraid to raise issues: they distinguish between honest mistakes and deliberate violations, support fair investigations, protect those who report in good faith, and demonstrate that the goal is to learn and improve, not to find a scapegoat. A simple example: an employee notices that they have accidentally sent a document to the wrong recipient. An ethical leader does not humiliate them, but helps them to quickly notify those responsible, minimise the damage, learn lessons and adjust the process so that the mistake is not repeated.

Ultimately, ethical leadership is a combination of a manager's personal integrity, their ability to establish fair rules of the game and to embed ethics into practical decisions, especially when there is pressure, uncertainty or a «grey area». Decision-making models help to make ethical choices systematic: they translate moral principles into understandable questions about compliance, consequences for people, fairness, transparency, and long-term trust. When a leader consistently uses such approaches and demonstrates them in their own actions, ethics ceases to be an abstract topic and becomes a practical skill of the organisation, reducing compliance risks and strengthening business resilience.

Common ethical dilemmas in the corporate environment arise where a formally permitted action may create hidden bias, injustice or the risk of losing trust. In practice, the dilemma does not usually look like an obvious violation of the law; more often it is a «borderline» situation where a person wants to be loyal to the company, maintain good relations with a partner, fulfil a plan, not lose a client or spoil relations with management. It is in such circumstances that the principles of integrity, transparency, fairness and compliance risk management become particularly important, as one wrong move can turn into a corruption incident, a reputational crisis or a violation of internal policies, even when the person had no intention of doing anything illegal.

Conflict of interest is one of the most common ethical dilemmas, as it can exist even without direct benefits «in an envelope». A conflict of interest arises when the personal interests of an employee or persons associated with them may influence, or appear to influence, the objectivity of their decisions in official matters. It is important to understand that the ethical problem lies not only in the actual influence, but also in the very possibility of bias and the impression this makes on others. A simple example is an employee who participates in the selection of a supplier and recommends a company

where a close relative works. Even if the price and quality are really good, the risk is that the decision may be perceived as «promoting one's own,» and the employee may unconsciously evaluate the documents more leniently or turn a blind eye to shortcomings. An even simpler example is a manager who has a personal friendship with a representative of a counterparty and may not notice red flags because «we've known each other for a long time and he's a decent person.» In such situations, the ethical decision is usually to openly declare the connection and remove oneself from the final decision or transfer it to another person or commission. This is not a punishment, but a way to protect both the employee and the organisation from suspicion and risk.

In a corporate environment, conflicts of interest often manifest themselves through «side» activities. For example, an employee may be engaged in private consulting activities in the same field as their employer and may use their work contacts or information for their own benefit. Even if they do not steal data directly, the situation itself creates a risk that clients or partners will not understand what role they are playing and who owns the results of their work. A simple example is an IT department employee who moonlights and offers the same client a «cheaper» option to do part of the work privately. Formally, it may be difficult to prove the damage immediately, but ethically, it undermines loyalty and fairness and may violate contractual obligations and confidentiality rules.

Gifts and hospitality are another classic area of ethical dilemmas, because in many cultures gifts are seen as a normal gesture of courtesy, but in a corporate context they can become a tool for influencing decisions. The main ethical problem here is that a gift or invitation can create a sense of obligation, even if the person did not plan to «repay» the favour. The psychological mechanism of reciprocity is very strong: when people receive something pleasant, they are more likely to agree, be lenient, and make decisions in favour of the giver. A simple example is when a supplier gives a manager an expensive gadget «for the holidays» and then, a few weeks later, asks them to «speed up the signing of the documents» or to be «less picky» about the quality of the delivery. The manager may sincerely believe that they will remain objective, but from an ethical and compliance perspective, the risk has already been created because an invisible dependency and impression of bias has arisen.

The dilemma with gifts often arises in a «grey area» when the cost is low or the gift is symbolic. For example, a partner gives a branded souvenir, a basket of sweets or flowers after the completion of a project. The ethical assessment here depends on the context. If this happens after all decisions have been made and the gift is symbolic, the risk of influence is lower. If the gift is given during a tender, negotiations or an audit, even a symbolic gesture can look like an attempt to influence. A simple example is a supplier inviting an employee who evaluates commercial proposals to dinner. Even if the bill is small, the situation itself undermines the neutrality of the process because it creates a private channel of influence and unequal conditions for other participants. That is why the ethical decision is often to refuse or postpone such hospitality until the decision-making process is complete, or to choose a format that

is transparent and does not create dependency, such as an official working lunch with several representatives from both sides and with expenses recorded.

Hospitality as a corporate practice can be legitimate when it has a clear business purpose and is proportionate. For example, a formal meeting with a partner in the format of a working lunch to discuss the terms of a contract may be acceptable in itself if the expenses are reasonable, the decision does not depend on «perks» and is made collegially and transparently. But hospitality becomes ethically problematic when its purpose is not communication but influence, when it is excessive or tied to a specific decision. A simple example is when a partner pays for travel, accommodation and entertainment for a manager and calls it a «study visit», although in reality the programme is almost entirely recreational and takes place just before the signing of a large contract. Even if the manager does not take any money, such «hospitality» has the characteristics of an undue advantage and creates a high risk of corruption.

The area of interaction with representatives of state bodies or state-owned enterprises is particularly sensitive. Here, even small gifts or treats can have a different legal and ethical meaning, as they create the suspicion that decisions can be «bought» through personal relationships. A simple example is when a company gives an official a «souvenir» during an inspection or document approval. Even if the souvenir is inexpensive, the timing and status of the recipient make the situation risky. An ethical approach would require avoiding such practices or acting exclusively within the limits of officially permitted protocols, where transparency and legality are beyond doubt.

Corporate ethical dilemmas in these areas are often exacerbated by pressure to perform. When employees are evaluated solely on financial results and speed, they may perceive gifts and informal agreements as a «business tool.» A simple example is a manager who believes that «without gifts, no one will buy from us in « or that «all competitors do it.» This is a typical moral rationalisation that shifts the ethical problem to the realm of «market reality.» Ethical management in such cases consists of the company clearly defining boundaries, providing safe alternatives, and supporting employees who refuse to engage in risky practices. If an employee refuses a questionable gift and temporarily loses a deal as a result, they should not be punished; otherwise, the organisation itself encourages misconduct.

Ultimately, conflicts of interest, gifts and hospitality are typical ethical dilemmas because they lie at the intersection of human psychology, business relationships and compliance risks. They rarely appear to be «black and white,» but it is in these «grey» situations that a culture of integrity is formed. A simple practical guideline is that an ethical decision must stand up to the test of context and perception: does it create dependency, does it influence or appear to influence objectivity, would it be comfortable to explain this decision to colleagues, an auditor or a client, and does it violate the fairness of the process? When an organisation trains employees to see these risks and supports them in making the right decisions, compliance ceases to be a formality and becomes a practice of trust that protects the business in the long term.

2.5. Globalisation of ethical standards and cross-cultural aspects of business ethics

The globalisation of economic activity has significantly changed the nature of ethical challenges faced by modern organisations. Companies increasingly operate in multiple countries simultaneously, collaborate with partners from different cultures, use global supply chains and engage international teams. In such an environment, ethical issues can no longer be considered solely within the framework of a single national legal system or cultural tradition. The globalisation of ethics means the formation of universal principles of responsible business conduct that are recognised in different countries and cultures, while leaving room for local social norms and business communication characteristics to be taken into account.

In modern international business practice, global standards of ethical behaviour are becoming increasingly important. They are shaped by international organisations, professional associations and global initiatives in the areas of sustainable development, anti-corruption, human rights protection and corporate responsibility. These standards create a common framework of expectations for how organisations should act, regardless of the country in which they operate. For example, international anti-corruption principles stipulate that a company should not provide undue benefits to officials, even in countries where informal payments have historically been a common practice. In such a situation, the global ethical standard takes precedence over local traditions and determines the behaviour of the organisation.

Case point. *Volkswagen Dieselgate. One of the most well-known examples of ethical and integrity violations in the European Union is the Volkswagen Dieselgate scandal, which occurred in Germany and generated international attention. In 2015, it was discovered that Volkswagen had installed specialised software in diesel vehicles to downplay emissions during laboratory tests, deliberately violating environmental laws and misleading regulators, consumers, and the public (European Commission, 2016; Ewing, 2017). Despite the presence of formal compliance structures, the case demonstrated a serious gap between the declared corporate values and the actual behaviour of the organisation. The resolution of the scandal involved litigation, significant fines and compensation, as well as significant changes to the company's corporate governance and compliance systems. As a result, Volkswagen suffered significant financial losses, reputational damage, and was forced to reconsider its approaches to ethics, control, and management responsibility. This case clearly demonstrates that the absence of a culture of integrity and responsibility can significantly reduce the effectiveness of formal compliance mechanisms, while their integration into corporate culture helps prevent misconduct.*

At the same time, the globalisation of ethics does not mean completely ignoring cultural differences. On the contrary, it requires an understanding that different societies have different traditions of communication, different forms of showing respect, and different ideas about hierarchy, collective responsibility, or individual initiative. A cross-cultural

perspective in ethics involves the ability to understand these differences without violating the fundamental principles of integrity, honesty, and legality. For example, in some countries, it is customary to give symbolic gifts during business meetings as a sign of hospitality and respect. In an international company, this can create an ethical dilemma, as in other jurisdictions even a small gift can be perceived as a potential tool for influencing decisions. In such a situation, the organisation must find a balance between cultural sensitivity and adherence to its own ethical standards. A simple solution may be a rule that gifts are only allowed if they are symbolic, transparent and registered in a special register.

Cross-cultural differences also manifest themselves in communication and decision-making styles. In some cultures, direct and frank communication is accepted, where people openly express disagreement or criticism. In other cultures, indirect communication prevails, where it is important to maintain harmony and avoid open conflict. This can affect the perception of ethical messages or compliance policies. For example, in an international team, an employee from a country where direct communication is accepted may openly report a problem or possible violation. Another employee from a culture where it is important to avoid confrontation may not dare to speak up about the problem directly so as not to put their colleague in an awkward position. In such a situation, the company should create safe and diverse communication channels, such as anonymous reporting platforms, so that every employee can express their concerns without cultural or psychological barriers.

The globalisation of ethics is also evident in issues of corporate social responsibility. Different countries may have different standards for working conditions, environmental protection, or interaction with local communities. However, international companies are increasingly applying the same ethical standards across all their divisions. For example, a company may require its suppliers to comply with the same rules prohibiting child labour or hazardous production conditions, regardless of whether local law requires it. A simple example can be seen in global clothing or electronics supply chains, where large international brands audit factories in different countries to ensure that workers are working in safe conditions and receiving fair wages.

Another important aspect of cross-cultural ethics is the issue of different attitudes towards hierarchy and authority. In some cultures, employees may directly address management and question decisions, while in other cultures such behaviour may be perceived as disrespectful. This can affect the functioning of compliance management systems, especially in the area of reporting violations. For example, in an international company, an employee from a country with a high regard for hierarchy may not report a problem if it involves the actions of a manager. They may feel that it is not their role or that it may appear disrespectful. In such a situation, the organisation must clearly communicate that reporting violations is part of professional responsibility and is not considered a sign of disloyalty.

A cross-cultural perspective on ethics also helps to avoid misunderstandings in international teams. For example, in some cultures, punctuality is seen as a strict norm and being late may be seen as disrespectful to a partner. In other cultures, time may be interpreted more flexibly. If an international team is unaware of these differences,

simple organisational issues can become a source of conflict or misinterpretation of behaviour. Ethical leadership in a global environment requires the development of cultural sensitivity, the ability to listen and understand other approaches without losing sight of basic principles of integrity.

Thus, the globalisation of ethics and cross-cultural perspectives are shaping a new reality for modern organisations, in which ethical standards must combine universal principles with respect for cultural diversity. Universal principles such as honesty, responsibility, transparency and respect for human rights create a common basis for an organisation's behaviour in any country. At the same time, understanding cultural differences helps to implement these principles in a way that is acceptable and effective in different social contexts. It is the combination of global standards and cultural sensitivity that enables organisations to develop sustainable ethical management systems that maintain the trust of partners, customers and society in a global environment.

2.6. Mechanisms for preventing and detecting fraud in the ethics and compliance system

Fraud prevention and detection in an organisation is part of a broader system of risk management, internal control and compliance management, which aims to protect the company's resources, maintain the trust of customers and partners, ensure the reliability of financial information and prevent legal and reputational consequences. Fraud in a corporate environment usually means deliberate actions or inaction aimed at obtaining unlawful benefits through deception, concealment of information, abuse of trust or manipulation of processes. It is important to understand that fraud can be committed by both employees and external parties, and sometimes by both parties, for example, when an employee colludes with a supplier or customer.

Preventing fraud begins with the realisation that the risk of fraud is not just a «problem of dishonest people» but also a consequence of conditions that create opportunities for abuse. The classic explanation is that fraud most often occurs when motivation or pressure, the opportunity to commit abuse, and the ability to internally justify one's behaviour are simultaneously present. In practice, this means that even a decent person may commit a violation if they feel strong financial pressure, see that controls are weak, and convince themselves that it is «temporary» or «the company will not suffer.» A simple example of such a situation can be imagined in cash discipline: an employee has access to cash and can discreetly take a small amount, planning to «return it after payday.» If cash control is formal and management rarely conducts reconciliations, this creates an opportunity, and psychological rationalisation makes the act «not so bad». That is why fraud prevention is not limited to punishment, but includes creating conditions where the opportunity for abuse is minimised.

A key element of prevention is the formation of a culture of integrity, where honesty and transparency are not just words, but a real norm. Culture works as an «invisible control»: if employees see that managers do not use double standards, that

violations are not hushed up, that ethical issues can be discussed without fear, then the motivation for fraud decreases and risky actions become more noticeable. A simple example of cultural influence: in a company where «everyone does it,» employees may consider it normal to take office supplies home or «pad» their timesheets. In a company with a clear culture of integrity, even minor abuses are seen as unacceptable, and employees are more likely to stop themselves or their colleagues.

Fraud prevention is closely linked to the organisation of internal controls, primarily the separation of duties, so that one person cannot single-handedly create, approve and execute a transaction and then cover up the traces. A simple example in procurement: if one employee can independently select a supplier, approve a contract, accept goods and confirm payment, there is a high probability of collusion or «front» suppliers. When the process is divided, for example, the selection of a supplier is carried out by a commission, the goods are accepted by the warehouse, and payment is made by the finance department based on confirmed documents, the possibility of fraud is significantly reduced. It is important that such controls are not only on paper but actually work, and this is where the difference between formal and effective control often arises.

Access management and digital control are particularly important, as a significant proportion of modern fraud is linked to information systems, databases and electronic payments. Prevention involves granting access on a «need-to-know» basis, regularly reviewing access rights, and monitoring changes in counterparty directories, bank details, prices, and nomenclature. A simple example: if an accountant can change a supplier's bank details without additional approval, a malicious actor can substitute the account and transfer funds to a third-party account. A preventive mechanism is to require double confirmation of changes, for example through a manager or independent financial control, and to record all changes in the system log.

Fraud detection is based on a combination of regular monitoring, data analytics, internal audits, and reliable reporting channels. Detection works when an organisation is able to notice deviations from the norm and quickly understand whether it is a mistake or a sign of intentional abuse. A simple example of analytical detection: if a company suddenly sees an increase in the proportion of purchases from a single supplier or frequent payments for small amounts that «break» approval limits, this could be a sign of fraud. Similarly, if an employee regularly conducts transactions at unusual times, such as late at night or on weekends, this may be a sign that they are trying to act inconspicuously. Such «signals» do not in themselves prove fraud, but they are grounds for investigation.

An extremely effective detection tool is the ability for employees and partners to report suspicious activity through secure channels. In many cases, fraud is uncovered precisely because of information from people who see the situation from the inside, rather than through a random audit. A simple example: an employee notices that their manager is asking them to sign off on work that was not actually done, or is asking them to «not ask unnecessary questions.» If the company has a secure reporting channel and a policy of protection against retaliation, the employee has a

chance to report the problem, and the organisation can stop the damage at an early stage. If the employee is afraid of retaliation or believes that «nothing will change anyway,» the fraud can continue for years.

Detecting fraud also requires high-quality work with documents and evidence, as it is important not only to «suspect» but also to gather information in such a way that it is suitable for internal investigation, disciplinary decisions or legal protection. A simple example: if a suspicious payment is detected, it is necessary to compare the contract, acts, invoices, correspondence, system data on approval, and actual confirmation of receipt of goods or services. It is the comparison of «what is documented» with «what actually happened» that allows one to distinguish between a mistake and a deliberate scheme.

Once a suspicion has been identified, the key is to respond correctly. An ineffective response, such as chaotic accusations without evidence or an attempt to «cover up» the problem, often causes more damage than the fraud itself, as it destroys trust and creates a sense of impunity. An effective response means carefully preserving evidence, temporarily restricting access, assessing the scale of the problem, conducting an internal investigation in confidence, taking proportionate measures and, if necessary, notifying law enforcement or regulatory authorities. A simple example of an adequate response: a company discovers that a supplier is billing for work that was not performed and suspects collusion with an employee. Instead of immediately accusing the person publicly, the company first blocks further payments, preserves documents, verifies the actual performance of the work, analyses correspondence and approval decisions, and then takes appropriate disciplinary and legal action.

Fraud prevention and detection are only effective when an organisation learns from its mistakes and improves its systems. After an incident, it is important not to stop at punishment, but to understand what gaps in controls allowed the scheme to occur. For example, if fraud was made possible because one person had too much authority, you need to change the distribution of functions, strengthen approvals, and set up audit logs and analytical triggers. If the problem arose due to unrealistic KPIs and pressure to «get it done at any cost,» the incentive system should be reviewed to ensure that it does not encourage circumvention of the rules. In the simple example of business trips, where employees were falsifying receipts, the company could implement an electronic expense tracking system with automatic checks, but it should also explain to employees that reimbursements must be honest and ensure that the business trip policy is realistic and does not force people to «bend the rules.»

Ultimately, fraud prevention and detection is a combination of a culture of integrity, well-designed processes and controls, access and data management, anomaly analytics, and secure reporting channels. Simply put, an organisation reduces the risk of fraud when it makes wrongdoing difficult, visible and unprofitable, and rightdoing understandable, supported and fairly rewarded. This is not only protection against losses, but also an investment in trust, stability and long-term business sustainability.

2.7. Developing and implementing effective ethics and compliance programmes

Developing an effective ethics and compliance programme means creating a system of rules, processes, roles and practices that simultaneously fosters a culture of integrity and ensures compliance with legislation and internal requirements. Effectiveness in this context is not limited to the existence of documents or formal procedures. It means that the programme has a real impact on people's behaviour, reduces risks, helps the organisation make better decisions, detects violations at an early stage and is able to substantiate its work with evidence when the company faces an audit, inspection, investigation or litigation. It is important that the ethics and compliance programme is «alive» and adaptive, i.e. it changes along with the business model, regulatory requirements, market risks and internal processes.

Such a programme begins with a clear identification of why it is needed for this particular organisation and what risks are most significant. The core of the programme will vary from company to company. For a bank, the key areas may be financial monitoring, AML/CFT, sanctions and data protection. For a trading company working with public procurement, the most critical risks are anti-corruption, conflicts of interest, tender transparency, and control of intermediaries. For an IT company, the priorities are often confidentiality, cybersecurity, intellectual property, and fair marketing practices. A simple example of risk logic: if a company often uses agents or intermediaries in international trade, the programme should be particularly strict in regulating the verification of third parties, commission payments, confirmation of services actually provided, and control of gifts and hospitality, because it is through intermediaries that illegal payments are most often «masked».

Next, the programme requires a clear definition of responsibility and independence of the function that supports it. Ethical and compliance rules do not work if they are «nobody's» or if the people who are supposed to control depend on those they control. An effective model provides for clear accountability to management and, where possible, to the supervisory level, so that the programme has authority and can stop risky decisions. A simple example of independence: if the compliance officer is dependent on the sales manager, who is pushing to meet the plan, compliance will be inclined to «miss» risky deals. If compliance has the right to escalate to the board or committee level, it can firmly say «this deal needs to be reviewed» and not fear the consequences for its own career.

The ethical part of the programme begins with formulating organisational values and translating them into understandable behaviour. Values should not sound like beautiful slogans, but rather like practical guidelines that help people in their daily decisions. For example, the value of «honesty» in working practice means not only «not lying,» but also not misleading the client with terms and conditions, not hiding risks, not manipulating reports, and not promising what will definitely not be delivered. The value of «respect» means zero tolerance for discrimination, proper communication, and protection of customer privacy. The value of «responsibility» means a willingness to admit mistakes and correct them, rather than shifting blame.

A simple example of practical translation: if a company declares «transparency,» then contracts must clearly explain what the price consists of, and there should be no hidden commissions or conditions in sales that the customer only learns about «after signing.»

The compliance part of the programme requires policies and procedures, but their effectiveness depends on how specific, understandable and applicable they are. A policy that is written in complex language and does not correspond to real processes does not work. Instead, documents that answer typical questions from employees in real situations work. A simple example is the policy on gifts and hospitality. It should explain what is considered a gift, what the limits are, when approval is required, how to record it in the register, what to do if it is awkward to refuse, and how to act during tenders or negotiations. If an employee receives a gift basket for a holiday, an effective procedure will tell them to notify compliance, enter it in the register, and, if necessary, transfer the gift for shared use or return it with a polite letter. This removes the stress of «how not to offend a partner» and at the same time protects the company.

In a mature programme, key risks are «embedded» in business processes so that compliance is not a separate bureaucracy but becomes part of normal operations. This means that control steps appear at the right points in the process: during onboarding of counterparties, conclusion of contracts, approval of payments, launch of marketing campaigns, hiring, access to data, and working with contractors. A simple example of integration: if a company pays a commission to an agent, the system should not allow payment without a package of documents confirming the actual services, without checking the agent, and without agreeing on increased risks. Employees should not have to «remember» about compliance; the process should make risky decisions impossible or at least noticeable.

An effective programme is impossible without training, but training must be practical and relevant to people's work. The basic mistake of many programmes is to treat training as a formality: a long presentation, a test «for the sake of it» and minimal behavioural change. Instead, short modules with realistic scenarios are needed, where employees see a situation, choose a solution, and receive an explanation of why. A simple example of scenario training: an employee receives a letter from a «supplier» requesting an urgent change of bank details for payment. The training shows that this is a typical fraud scheme and teaches employees to call back the official number, verify the details through an independent source, and approve changes according to procedure. Such training immediately reduces the risk of losses.

A critically important part of the programme is the mechanism for reporting violations and internal consultations, because ethics and compliance are most often «broken» when an employee does not know how to act or is afraid to raise the issue. An effective programme creates safe channels where people can ask questions before making a mistake or report an incident without fear of retaliation. A simple example: an employee suspects a conflict of interest in procurement but has no evidence.

If the company has a reporting channel and a protection policy, the employee can pass on the information, and compliance will initiate an investigation discreetly and professionally, without turning it into a public conflict.

Separately, the programme must include monitoring and measurability, otherwise the organisation will not know if it is actually working. Monitoring does not mean total control of every step, but rather regular observation of key indicators, analysis of incidents, verification of high-risk processes, and assessment of how behaviour is changing. A simple example of useful measurability: a company tracks how many requests for compliance advice it receives from the business, how many incidents are reported, what types of violations are recurring, how long investigations take, whether there are delays in counterparty checks, and whether the number of exceptions to procedures is increasing. If they see an increase in the number of «exceptions» in procurement, this is a signal of either excessive bureaucracy or attempts to circumvent controls, and the programme must respond.

The effectiveness of the programme also depends on how the organisation responds to violations. If violations are hushed up, if punishment is selective or depends on a person's status, if no lessons are learned from incidents, then the programme becomes decorative. Instead, an effective programme has fair discipline and corrective measures: employees must understand that the rules are real, but at the same time there must be a distinction between deliberate fraud and a bona fide mistake. A simple example of fairness: if an employee accidentally violated a procedure due to ignorance, the company can provide training, change the process, and issue a warning, but if an employee deliberately concealed information or falsified documents, the response must be more severe, otherwise the culture of integrity will be destroyed.

Finally, the ethics and compliance programme must be constantly reviewed and improved as risks change. New regulatory requirements, new fraud schemes, new digital threats, new markets and partners are emerging. A simple example of adaptation: the company started working with international payments, and previously, sanctions screening was not necessary. After entering new markets, it becomes necessary to check counterparties, ultimate beneficiaries, countries of origin, and correspondent banks. The programme must add procedures, configure tools, and train people, otherwise the risk of sanctions violations will become critical.

Ultimately, an effective ethics and compliance programme is a system that combines values and behavioural standards with specific policies, processes, training, monitoring, and fair response to incidents. It works when employees understand not only «what is prohibited» but also «why it is important,» when managers set a consistent example, when control mechanisms are built into processes, and when people have safe tools for questions and reports. Simply put, it is a programme that makes ethical behaviour the norm, risky decisions visible, and violations quickly detected and addressed, while helping the organisation grow legally, steadily, and with the trust of society and partners.

Practical Exercises

Exercise 1 – Identifying the Core Concepts of Ethics, Integrity, Compliance, and GRC

Scenario:

A medium-sized manufacturing company is revising its internal governance framework after several cases of inconsistent decision-making, unclear accountability, and weak ethical oversight.

Tasks:

> Identify the conceptual differences between ethics, integrity, compliance, governance, and risk management.

> Explain how these elements interact within the broader GRC framework.

> Suggest two practical risks for an organisation when these concepts are treated as separate "parallel worlds" rather than as an integrated system.

Exercise 2 – Distinguishing Ethics-Based and Compliance-Based Approaches

Scenario:

A company has introduced several compliance procedures, but employees still perceive ethical issues as "formalities" and often look for loopholes in the rules.

Tasks:

> Describe the differences between an integrity-based approach and a compliance-based approach to managing behaviour.

> Provide one example of a situation where compliance alone may be insufficient, but ethics provides the correct guidance.

> Evaluate why organisations need both approaches in order to build a sustainable ethical culture.

Exercise 3 – Designing an Organisational Values Module

Tasks:

> Draft three key messages for a short internal awareness session explaining the relationship between values, rules, and laws.

> Define two examples of how organisational values can be translated into everyday employee behaviour.

> Propose one method for assessing whether declared corporate values are actually reflected in practice.

Exercise 4 – Analysing Behavioural Ethics and Misconduct Risks

Scenario:

An employee bypasses part of the procurement verification process, justifying it as "saving time" and claiming that "everyone does it this way."

Tasks:

> Identify the behavioural and psychological factors involved in this case, such as rationalisation, social pressure, conflict of interest, or gradual normalisation of deviance.

> Explain how such minor deviations can evolve into larger misconduct risks.

> Suggest two organisational measures that could reduce the likelihood of this type of behaviour.

Exercise 5 – Applying Ethical Decision-Making Models

Scenario:

A supplier offers hospitality to a procurement manager during an active tender process. The offer is not explicitly prohibited by company policy, but it may influence perception of neutrality.

Tasks:

> Apply two ethical decision-making models from the text, such as the legal/compliance test, fairness test, consequence model, or publicity test.

> Decide whether the hospitality should be accepted, declined, or postponed, and justify your answer.

> Explain why "formally allowed" does not always mean "ethically appropriate".

Exercise 6 – Managing Conflicts of Interest, Gifts, and Hospitality

Scenario:

A project manager participates in the selection of a supplier whose representative is a close personal friend. At the same time, the supplier has sent symbolic gifts to several members of the team.

Tasks:

> Identify the ethical and compliance risks in this situation.

> Explain how the organisation should distinguish between acceptable courtesy and a situation that creates real or perceived bias.

> Recommend practical steps the organisation should take to manage the conflict of interest and protect the fairness of the process.

Exercise 7 – Cross-Cultural Ethics in International Business

Scenario:

An international company operates in several countries where business customs differ significantly, especially in relation to hierarchy, gift-giving, and communication style.

Tasks:

> Explain how global ethical standards can coexist with cross-cultural differences in business practice.

> Provide one example of a local custom that may create an ethical dilemma for a multinational organisation.

> Evaluate how the company can remain culturally sensitive without compromising integrity, legality, and anti-corruption standards.

Exercise 8 – Preventing and Detecting Fraud

Scenario:

An internal audit reveals repeated small payments to one supplier just below approval thresholds. No direct proof of fraud is available yet, but the pattern looks unusual.

Tasks:

> Identify the possible fraud indicators and explain why they should be treated as warning signals.

> Describe how the organisation should combine internal controls, data monitoring, reporting channels, and investigation procedures in response to this case.

> Suggest two preventive measures that could reduce similar fraud risks in the future.

Exercise 9 – Building Ethical Leadership and Speak-Up Culture

Scenario:

Employee interviews show that staff members are reluctant to raise concerns because they believe managers care more about results than about fairness or integrity.

Tasks:

> Identify leadership behaviours that support ethical culture and reduce misconduct risks.

> Propose three actions managers can take to demonstrate consistency, fairness, and openness to concerns.

> Suggest how the organisation can measure whether employees feel psychologically safe to ask questions or report problems.

Exercise 10 – Developing an Ethics and Compliance Programme (Final Project)

Scenario:

Your team acts as an internal task force responsible for designing an ethics and compliance programme for a Ukrainian company seeking to strengthen corporate integrity, improve fraud prevention, and align its practices with international standards such as ISO 37301, ISO 37302, and ISO 37001.

Tasks:

> Map out the main components of the programme: values, code of conduct, policies, training, reporting channels, monitoring, internal controls, investigations, and corrective actions.

> Develop an implementation roadmap that includes phases, responsible functions, communication actions, and key performance indicators.

> Present your roadmap as a short policy briefing, explaining how the programme supports ethical behaviour, trust, legal compliance, and long-term organisational sustainability.

Target Questions

1. What is the role of business ethics in shaping responsible organisational behaviour in the international business environment?
2. What are the key differences and complementarities between integrity-based and compliance-based approaches to managing corporate ethical behaviour?
3. How do international standards and European Union regulations contribute to the institutionalisation of ethical principles and the mitigation of the risks of misconduct in business?

4. What conclusions about the role of corporate culture and management responsibility can be drawn from the European Union case studies, particularly Volkswagen Dieselgate and the whistleblowing incidents?
5. How can integrating a values-oriented approach and effective compliance mechanisms enhance the sustainability, transparency, and trust of organisations in the long term?
6. How do governance, risk management, compliance, and ethics interact within the broader GRC framework in modern organisations?
7. What is the significance of organisational values in shaping ethical behaviour and supporting compliance with internal rules and external legal requirements?
8. How do values, rules, and laws differ in their regulatory function, and why is their alignment important for an effective ethics and compliance system?
9. What psychological and behavioural factors contribute to misconduct in organisations, and how can they be addressed through ethics and compliance management?
10. How do rationalisation, social pressure, conflicts of interest, and the gradual shift in norms influence employees' unethical behaviour?
11. What is the role of ethical leadership in preventing misconduct and promoting a culture of integrity in the corporate environment?
12. How can ethical decision-making models help managers and employees address dilemmas in "grey areas" where formal rules alone are insufficient?
13. Why are conflicts of interest, gifts, and hospitality considered high-risk areas in corporate ethics and compliance?
14. How can organisations distinguish between culturally acceptable business practices and conduct that may create corruption or integrity risks?
15. In what ways does globalisation influence the development of universal ethical standards while still requiring sensitivity to cross-cultural differences?
16. How do cross-cultural differences in communication, hierarchy, and decision-making affect the implementation of ethics and compliance programmes in international organisations?
17. What mechanisms are most effective for preventing and detecting fraud within an ethics and compliance system?
18. How do internal controls, reporting channels, data monitoring, and organisational culture contribute to fraud prevention and early detection?
19. What are the essential components of an effective ethics and compliance programme in contemporary organisations?
20. How can organisations ensure that ethics and compliance programmes remain practical, risk-based, and adaptable to changing business and regulatory environments?
21. Why is employee training, safe reporting mechanisms, and fair response to violations critical for the effectiveness of ethics and compliance programmes?
22. How can organisations move from a formal "check-box" approach to compliance towards a living culture of integrity and ethical responsibility?

References for Self-study

1. Blessing, M. (2024). *Regulatory Compliance and Ethical Considerations*.

2. Federal Ministry of Justice. (2023). *Hinweisgeberschutzgesetz (Whistleblower Protection Act)*. Federal Ministry of Justice. https://www.gesetze-im-internet.de/hinschg/

3. European Commission. (2016). *Emissions in the automotive sector*. European Commission. https://single-market-economy.ec.europa.eu/sectors/automotive-industry/environmental-protection/emissions-automotive-sector_en

4. European Commission. (2023). *Corporate sustainability due diligence*. European Commission. https://commission.europa.eu/business-economy-euro/doing-business-eu/corporate-sustainability-due-diligence_en

5. European Union. (2019). *Directive (EU) 2019/1937 of the European Parliament and of the Council on the protection of persons who report breaches of Union law*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2019/1937/oj

6. Ewing, J. (2017). *Faster, higher, farther: The Volkswagen scandal*. TRANSWORLD PUBLISHERS. https://archive.org/details/fasterhigherfart0000ewin_e5z6/page/n6/mode/1up

7. Geddes, B. (2017). Integrity or Compliance Based Ethics: Which Is Better for Today's Business? *Open Journal of Business and Management*, *05*, 420–429. https://doi.org/10.4236/ojbm.2017.53036

8. Geddes, B.H. (2017) Integrity or Compliance Based Ethics: Which Is Better for Today's Business? Open Journal of Business and Management, 5, 420-429. https://doi.org/10.4236/ojbm.2017.53036

9. Government Commission German Corporate Governance Code. (2022). *German Corporate Governance Code*. Government Commission German Corporate Governance Code. https://www.dcgk.de/en/code//foreword.html

10. Gross-Schaefer, Arthur, Cueto, A. Cathleen (2017). Ethics & Compliance: The Game-Changer in the Business World. International Journal of Business and Social Science. Vol. 8, No. 2, 57-65. https://ijbss.thebrpi.org/journals/Vol_8_No_2_February_2017/8.pdf

11. International Organization for Standardization. (2021). *ISO 37301: Compliance management systems - Requirements with guidance for use*. International Organization for Standardization. https://www.iso.org/standard/75080.html

12. Jacobs, D. C. (2004). A Pragmatist Approach to Integrity in Business Ethics. *Journal of Management Inquiry*, *13*(3), 215–223. https://doi.org/10.1177/1056492604268203

13. Lartey Franklin M. (2021). Integrity-based and Compliance-Based Ethics Programmes: A Critical Analysis of Key Differences. International Journal of Economics, Business and Management Research, Vol. 5, No. 5, 43–53. https://www.ijebmr.com/uploads/pdf/archivepdf/2021/IJEBMR_739.pdf

14. Roberts, R. (2009). The Rise of Compliance-Based Ethics Management. *Public Integrity*, *11*(3), 261–278. https://doi.org/10.2753/PIN1099-9922110305

15. Tullberg, J. (2012). Integrity - Clarifying and Upgrading an Important Concept for Business Ethics. *Business and Society Review*, *117*(1), 89–121. https://doi.org/10.1111/j.1467-8594.2011.00401.x

16. United Nations Global Compact. (2023). *The ten principles of the UN Global Compact*. United Nations Global Compact. https://www.unglobalcompact.org/what-is-gc/mission/principles

17. Weber, J., & Wasieleski, D. M. (2013). Corporate Ethics and Compliance Programs: A Report, Analysis and Critique. *Journal of Business Ethics*, *112*(4), 609–626. https://doi.org/10.1007/s10551-012-1561-6

Assignments for Self-Study

1. *Essay: Ethics, Integrity and Compliance in Modern Organisations.* Analyze the conceptual differences between business ethics, integrity, and compliance. Explain why compliance cannot be limited only to formal adherence to laws, rules, and internal procedures. Discuss how integrity and ethical values help organisations make responsible decisions in “grey areas” where the law or policy does not provide a clear answer. Provide practical examples related to gifts, conflicts of interest, customer communication, or counterparty verification.

2. *Mini-Case Study: Ethical Failure and Compliance Breakdown.* Choose a Ukrainian or international case involving ethical misconduct, fraud, corruption, environmental manipulation, or weak compliance culture. Possible examples include Volkswagen Dieselgate, Wirecard, Enron, Siemens corruption scandal, or a Ukrainian public procurement/corporate governance case. Identify the main ethical and compliance failures in the case. Evaluate whether the organisation had formal compliance mechanisms and why they failed to prevent misconduct. Discuss the role of corporate culture, leadership, incentives, and internal controls. Propose lessons that Ukrainian organisations can adapt to strengthen ethical behaviour and compliance management.

3. *Comparative Table: Ethics, Compliance, Governance, Risk Management and GRC.* Prepare a comparative table explaining the differences between ethics, compliance, governance, risk management, and GRC. Compare them according to the following criteria: main purpose, key focus, source of requirements, responsible actors, tools and procedures, and practical examples. Highlight how these concepts complement each other in an integrated management system. Explain why compliance may become formal and ineffective if it is not supported by ethical culture and risk-oriented governance.

4. *Interview Assignment: Ethical Culture and Decision-Making in Organisations.* Conduct a short interview with a compliance officer, internal auditor, HR manager, legal specialist, manager, or accountant. Ask what ethical dilemmas employees most often face in practice, what encourages or discourages ethical behaviour, how conflicts of interest are managed, and whether employees feel safe reporting concerns.

Summarize the key insights and reflect on how organisational values, leadership behaviour, and internal rules influence everyday ethical decision-making.

5. *Practical Task: Designing a Code of Ethics and Compliance Rules.* Develop a short Code of Ethics and Compliance Rules for a fictional organisation. The document should include: core values, principles of honesty, fairness, responsibility, transparency and integrity, rules on conflicts of interest, gifts and hospitality, confidentiality, responsible use of company resources, reporting concerns, and consequences of violations. Ensure that the code combines both a values-based approach and a compliance-based approach, showing not only what is prohibited but also what ethical behaviour is expected from employees and managers.

6. *Applied Research: International Standards and Corporate Ethics Programmes.* Select one international or European framework related to ethics and compliance, such as ISO 37301 Compliance Management Systems, ISO 37001 Anti-Bribery Management Systems, OECD Guidelines for Multinational Enterprises, UN Global Compact, or the EU Whistleblower Protection Directive. Summarize its main requirements or principles for organisations. Compare these requirements with the idea of an effective ethics and compliance programme described in the study material. Explain how Ukrainian organisations could use this framework to improve corporate integrity, prevent misconduct, and strengthen stakeholder trust.

7. *Essay: Behavioural Ethics and the Psychology of Misconduct.* Explain why misconduct in organisations is often caused not only by "bad people," but also by psychological factors and organisational conditions. Analyze the role of rationalisation, social pressure, conflict of interest, gradual shift of norms, diffusion of responsibility, and performance pressure. Provide examples of how ordinary employees may justify unethical behaviour, such as bypassing procedures, manipulating reports, accepting questionable gifts, or ignoring red flags. Suggest how organisations can reduce these risks through ethical leadership, training, incentives, internal controls, and open communication.

8. *Practical Task: Fraud Prevention and Detection Plan.* Design a short fraud prevention and detection plan for a company. Include key preventive mechanisms such as segregation of duties, access control, due diligence of counterparties, approval procedures, gift registers, internal audits, data monitoring, and secure reporting channels. Explain how the organisation should respond when fraud is suspected: preservation of evidence, confidential investigation, temporary restriction of access, disciplinary measures, legal action, and improvement of internal controls after the incident.

9. *Mini-Case Reflection: Ethical Leadership in a Grey Area.* Create or choose a short situation involving an ethical dilemma: for example, pressure to close a risky deal, receiving a gift during negotiations, choosing a supplier connected to a relative, manipulating performance indicators, or hiding an operational mistake. Apply at least three ethical decision-making tests: legality test, values/integrity test, consequences for stakeholders, fairness test, and publicity test. Explain what

an ethical leader should do and how their behaviour influences organisational trust and accountability.

10. *Comparative Reflection: Global and Cross-Cultural Business Ethics.* Analyze how globalisation influences business ethics and compliance. Discuss why international companies need universal ethical standards while also taking cultural differences into account. Use examples related to gifts, hierarchy, communication styles, reporting violations, labour standards, environmental responsibility, or supplier audits. Explain how organisations can remain culturally sensitive without compromising integrity, legality, transparency, and respect for human rights.

Chapter 3: Legal Frameworks and International Compliance Standards

Learning Outcomes

By the end of this chapter, students will be able to:

- > Explain the main international compliance standards, laws, and regulatory frameworks shaping corporate governance and risk management.
- > Compare EU and Ukrainian compliance systems, identifying similarities, differences, and areas of convergence.
- > Apply theoretical models and real-world case studies to evaluate compliance risks and design appropriate mitigation strategies.

Key Words: Compliance, Regulation, Governance, Due Diligence, Legal Liability, Risk Management, International Standards

Main Definitions

Compliance – The process of ensuring that organizational activities meet legal, regulatory, and ethical obligations (Parker, 2022).

Governance – The system of rules, practices, and processes by which an organization is directed and controlled (Baldwin, Cave, & Lodge, 2012).

Regulatory Risk – The potential for financial loss or reputational harm due to non-compliance with laws or regulations (Braithwaite, 2011).

Due Diligence – A systematic process of investigating and assessing compliance, financial, and operational risks before entering into business relationships or transactions (OECD, 2023).

Whistleblower Protection – Legal mechanisms that safeguard individuals who report misconduct from retaliation (European Commission, 2023).

Corporate Liability – The legal responsibility of a corporation for unlawful acts committed by its employees, agents, or executives within the scope of their duties (Coffee, 2020).

Compliance Management System (CMS) – A structured set of processes and controls designed to ensure adherence to applicable laws, regulations, and internal policies (ISO, 2021).

Risk-Based Approach – A principle of compliance management that prioritizes resources and controls based on the level of identified risk (Kaptein, 2015).

Anti-Money Laundering (AML) – Laws and processes aimed at preventing the concealment of the origins of illegally obtained funds (FATF, 2022).

Transparency – The practice of disclosing relevant, accurate, and timely information

about organizational operations and decision-making to stakeholders (Transparency International, 2023).

Standards, Laws, and Regulations

1. International*:* ISO 37301:2021 (Compliance Management Systems), OECD Guidelines for Multinational Enterprises, UN Convention Against Corruption (UNCAC).

2. European Union: GDPR (General Data Protection Regulation), EU Whistleblower Protection Directive (2019/1937), Anti-Money Laundering Directives (4–6).

3. Ukraine: Law of Ukraine "On Prevention of Corruption," Law "On Personal Data Protection," NABU regulations and High Anti-Corruption Court procedures.

List of Subchapters

3.1 Overview of Legal and Compliance Systems
3.2 International Compliance Standards (ISO, OECD, UN)
3.3 EU Compliance Frameworks and Case Law
3.4 Ukrainian Legal Landscape and Reforms
3.5 Risk Management and Compliance Programs
3.6 Comparative Analysis: EU vs. Ukrainian Standards
3.7 Emerging Trends and Future Challenges

3.1 Overview of Legal and Compliance Systems

Compliance frameworks have developed over the past several decades as a response to globalization, repeated corporate scandals, and an increasing demand from society for transparency and accountability (Baldwin, Cave, & Lodge, 2012; OECD, 2023). Scholars such as Parker (2022) and Braithwaite (2011) have argued that compliance systems should not only ensure adherence to legal rules but also cultivate an ethical organizational culture that encourages responsible decision-making. This approach allows organizations to move beyond reactive compliance toward proactive risk management and trust-building.

In the field of international business, compliance becomes even more critical. Cross-border operations are shaped by a wide range of rules, standards, and norms developed by both states and international organizations. Expanding into foreign markets requires companies to broaden their institutional environment and integrate legal obligations, regulatory expectations, and cultural considerations from multiple jurisdictions (Bradford, 2020; North, 1990). This includes understanding the legal traditions of partner countries, the standards of international trade, and the political and economic relationships that govern business at the interstate level.

The institutions that make up the external environment of international business are

diverse. They include foreign economic relations institutions, which govern how national economies interact with global markets (WTO, 2022), and international law, which provides a framework for property rights, contract enforcement, and dispute resolution (Schaffer, Agusti, & Dhooge, 2021). Labor and human rights standards developed by bodies such as the International Labour Organization (ILO, 2022) ensure fair working conditions and protect against exploitation, while market and financial institutions regulate taxation, credit, and monetary policy, shaping the business climate (IMF, 2023). International organizations such as the OECD, WTO, and United Nations create platforms for policy coordination and standard-setting, reducing uncertainty for companies operating globally (OECD, 2023). Cultural and social institutions also play a significant role, establishing both formal and informal norms that affect negotiation styles, management practices, and organizational behaviour (Hofstede, Hofstede, & Minkov, 2010).

Together, these legal, economic, and cultural institutions form the compliance ecosystem in which international companies operate. Navigating this environment requires more than technical knowledge of regulations. It calls for an integrated approach that combines legal expertise, risk management, and cultural intelligence, enabling businesses to meet their obligations, maintain stakeholder trust, and remain competitive in an interconnected global economy.

Relationship between law, compliance, and corporate governance

The modern global business environment is shaped by a triad of legislation, compliance, and corporate governance - an integrated system where each element reinforces the others to support sustainable management.

Legislation provides the framework by setting mandatory rules, defining permissible conduct, and establishing sanctions. Its effectiveness, however, depends on mechanisms for enforcement and monitoring.

Compliance acts as the bridge between external legal demands and internal management processes. Contemporary scholarship views it not only as risk management but as a proactive business philosophy grounded in legality, ethics, and responsible behaviour (Parker, 2022; Kaptein, 2015). Modern compliance programs include risk assessment, internal controls, employee training, and the promotion of a culture of integrity and accountability.

Corporate governance integrates legal obligations and compliance measures into a strategic system focused on long-term value creation for stakeholders (Baldwin, Cave, & Lodge, 2012). Governance shapes how compliance is organized and, in turn, responds to evolving legislation.

Maintaining balance is crucial: overly formalistic compliance can create bureaucratic rigidity, while weak compliance exposes firms to legal and reputational risks. In a globalized economy, companies must meet multi-jurisdictional requirements, adapt to standards such as ISO 37301, and respect diverse legal traditions (OECD, 2023).

Thus, the relationship between legislation, compliance, and corporate governance is best understood not as a simple sum of parts but as an integrated management framework. Together, they form the institutional backbone that enables companies to operate

responsibly, remain competitive, and achieve sustainable development in an increasingly complex and dynamic legal environment.

3.2 International Compliance Standards (ISO, OECD, UN)

International compliance standards create a shared framework for responsible conduct and risk management, helping organizations meet global expectations and reduce regulatory uncertainty. Three major frameworks shape this landscape: ISO 37301, the OECD Guidelines, and UNCAC.

ISO 37301:2021 defines requirements for Compliance Management Systems, stressing leadership commitment, risk-based controls, and continual improvement (ISO, 2021). Many EU firms, including Siemens, use ISO 37301 to integrate compliance into governance, and Ukrainian banks and energy firms are adopting it to meet EU expectations (KPMG, 2022).

The OECD Guidelines (2023) provide non-binding recommendations on human rights, labour, environment, and anti-bribery. They promote supply chain due diligence and align with EU efforts like the Corporate Sustainability Due Diligence Directive (European Commission, 2023). Ukraine has applied these guidelines to reform state-owned enterprise governance (OECD, 2022).

UNCAC, the only legally binding global anti-corruption treaty, obliges states to implement preventive measures, criminalize bribery and money laundering, and recover stolen assets (UNODC, 2019). Ukraine has enforced UNCAC through NABU and the High Anti-Corruption Court, raising prosecution rates for top-level corruption (Council of Europe, 2021).

Together, these frameworks push companies beyond “box-ticking” toward embedding integrity in corporate culture (Parker, 2022), boosting investor confidence, easing EU market access, and strengthening resilience.

3.3 EU Compliance Frameworks and Case Law

Global business operates within an increasingly dense network of national, regional, and international regulations, requiring companies to build compliance systems that manage overlapping and sometimes conflicting obligations (Bradford, 2020; Vogel, 2018). The U.S. regime is highly influential, combining detailed statutory requirements with strict enforcement (Coffee, 2020).

The Sarbanes–Oxley Act (SOX) of 2002 responded to scandals like Enron and WorldCom by strengthening corporate accountability. It mandates executive certification of financial statements (Sec. 302), independent audit committees, and internal control assessments with auditor attestation (Sec. 404), applying to all U.S.-listed firms, including foreign issuers (Coates, 2007). The Foreign Corrupt Practices Act (FCPA) of 1977 remains the leading global anti-bribery statute, prohibiting payments to foreign

officials and requiring accurate books and internal controls. Its extraterritorial scope covers U.S. and foreign issuers, with enforcement resulting in multibillion-dollar settlements (Spalding, 2011; DOJ, 2023). Together, SOX and FCPA have elevated compliance to a strategic management function and inspired reforms worldwide.

HIPAA establishes U.S. standards for patient health information, requiring administrative, technical, and physical safeguards, granting patients data rights, and imposing fines up to $1.5M annually for violations (HHS, 2023).

The EU model emphasizes harmonization and stakeholder rights. The General Data Protection Regulation (GDPR) sets strict principles—lawfulness, transparency, purpose limitation, and accountability—granting EU citizens rights such as data access, erasure, and portability. Non-compliance can result in fines up to 4% of global turnover, with penalties exceeding €2.8B since 2018, including a €746M fine against Amazon (European Commission, 2018; EDPB, 2022). MiFID II strengthens transparency, bans conflict-inducing inducements, and requires transaction reporting within one business day (ESMA, 2023). The Whistleblower Protection Directive (2019/1937) mandates secure reporting channels for organizations with 50+ employees and prohibits retaliation, prompting firms to strengthen internal investigations (European Commission, 2023).

The Asia-Pacific region presents diverse approaches: China's Cybersecurity Law, PIPL, and Data Security Act form a strict digital security triad, requiring local data storage and security assessments, with penalties up to 5% of turnover. Singapore's PDPA sets nine data protection principles, mandates breach notifications, and imposes fines up to 10% of annual turnover (PDPC, 2020). Australia's Corporations Act enforces "comply or explain" governance, continuous disclosure obligations, and significant penalties, with ASIC pursuing record enforcement actions in 2023.

To navigate this complex landscape, multinationals require layered compliance programs, constant monitoring of legal change, and adaptation to cultural contexts.

Case in Point: *Meta Ireland – Data Transfer Violation The Irish Data Protection Commission fined Meta €1.2 billion, emphasizing the importance of compliance with data transfer requirements under GDPR (EDPB, 2023).*

3.4 Ukrainian Legal Landscape and Reforms

Ukraine's legal and compliance architecture has been undergoing a profound transformation since 2014, a process that has accelerated in response to both internal and external pressures. The post-2014 era is characterized by an explicit commitment to transparency, rule of law, and European integration, driven in part by Ukraine's Association Agreement with the European Union (EU). This period marks a decisive shift away from fragmented, reactive compliance mechanisms toward the creation of a comprehensive, rule-based framework that aligns with international best practices (European Commission, 2023).

From an academic perspective, these reforms are not merely technical adjustments; they represent a paradigmatic shift in Ukraine's approach to governance. As Braithwaite (2011) argues in his theory of responsive regulation, the creation of robust enforcement

institutions, coupled with the adoption of preventive compliance measures, signals a transition from punitive, post-facto regulation to a preventive and systemic model of compliance management.

Anti-Corruption Legislation and Institutional Architecture

At the heart of Ukraine's compliance reform is the Law of Ukraine "On Prevention of Corruption" (2014), which has fundamentally reshaped the institutional landscape. This law established:

The National Agency on Corruption Prevention (NACP), responsible for policy development, oversight of asset declarations, and monitoring conflicts of interest.

The National Anti-Corruption Bureau of Ukraine (NABU), tasked with investigating high-level corruption, particularly in the public sector.

The creation of these institutions represents a significant application of what Baldwin, Cave, and Lodge (2012) call the "regulatory state," wherein specialized bodies are empowered with investigatory and sanctioning authority. By mandating electronic asset declarations for public officials, the law has introduced a mechanism of transparency that enables public and civil society oversight — an essential feature in a country historically plagued by opaque governance (Transparency International Ukraine, 2023).

Judicial Reform: The High Anti-Corruption Court

The establishment of the High Anti-Corruption Court (HACC) in 2019 has been hailed as a milestone in Ukraine's judicial reform agenda. The HACC provides a dedicated venue for the adjudication of corruption cases investigated by NABU and prosecuted by the Specialized Anti-Corruption Prosecutor's Office (SAPO). The court's composition — including judges vetted through a process involving international experts — has been praised by the Council of Europe (2021) as a model for ensuring independence and impartiality in high-profile cases.

From a compliance theory standpoint, the creation of HACC strengthens the "credible threat" component of enforcement: when corporate and public-sector actors know that high-level corruption cases will be prosecuted and adjudicated in a specialized, competent forum, the deterrent effect increases.

Data Protection and EU Alignment

Ukraine's Law on Personal Data Protection is currently undergoing substantial revision to harmonize with the EU's General Data Protection Regulation (GDPR). The forthcoming amendments will introduce stricter rules on data subject consent, mandatory breach notifications, and expanded enforcement powers for the national data protection authority (UNDP Ukraine, 2023). This alignment will reduce legal fragmentation for companies operating in both Ukrainian and EU jurisdictions and is expected to enhance Ukraine's attractiveness as a business environment.

Corporate Governance and SOE Reform

Another key element of Ukraine's compliance landscape is the reform of state-owned enterprises (SOEs). Following OECD recommendations, many SOEs have adopted supervisory boards with independent directors, improving transparency and insulating

decision-making from political interference (OECD, 2022). This is a classic application of corporate governance theory: separating ownership and control to reduce agency problems and improve performance.

Case in Point: NABU vs. State-Owned Enterprise Manager

In 2022, NABU investigated a large-scale embezzlement scheme within a state energy enterprise, where inflated procurement contracts had siphoned millions of hryvnias from the state budget. The case resulted in criminal prosecution, suspension of contracts, and partial recovery of funds (NABU, 2022).

This case illustrates the practical impact of Ukraine's compliance infrastructure. For students, it offers a clear example of how institutional reforms translate into enforcement capacity, and how that capacity can directly influence corporate behaviour and public trust.

Implications for Business and Governance

For corporate actors, these reforms create both opportunities and obligations. On one hand, the modernization of Ukraine's legal framework improves predictability, reduces corruption-related risks, and strengthens investor confidence. On the other hand, companies must now implement internal compliance programs, conduct thorough due diligence on counterparties, and prepare for more stringent enforcement.

From a governance perspective, the Ukrainian case demonstrates a transition from informal, relationship-based regulation toward a formalized, institution-driven compliance environment. This transition aligns with Parker's (2022) argument that compliance should evolve from mere rule-following into a driver of ethical corporate culture.

3.5 Risk Management and Compliance Programs

Risk management and compliance are closely intertwined disciplines that form the backbone of corporate governance. An effective compliance program is not simply a set of documents or procedures; rather, it is a dynamic system designed to identify, assess, mitigate, and monitor risks across the entire organization (ISO, 2021). This cyclical process ensures that risks are managed proactively rather than reactively and that compliance obligations are embedded into the organization's strategy and daily operations.

The Risk Management Cycle

According to ISO 37301:2021 and ISO 31000:2018, a robust compliance risk management system involves four iterative stages:

Risk Identification – Mapping potential compliance risks across legal, operational, financial, and reputational dimensions. For example, identifying exposure to anti-bribery risks in high-risk markets or data privacy risks when handling EU citizens' data (ISO, 2021).

Risk Assessment – Evaluating the likelihood and potential impact of each risk. This may involve quantitative scoring (e.g., risk heat maps) or qualitative judgment informed by expert input (Kaptein, 2015).

Risk Mitigation – Implementing controls, policies, and training programs to reduce identified risks. Mitigation may include adopting due diligence procedures, automating compliance checks, or restructuring approval workflows.

Risk Monitoring and Review – Continuously monitoring compliance indicators, auditing internal processes, and revising policies as regulations evolve (OECD, 2023).

This iterative approach aligns with Braithwaite's (2011) regulatory pyramid, which suggests that compliance programs should be responsive — escalating controls and interventions as risk levels increase.

Key Components of Effective Compliance Programs

A mature compliance program integrates the following elements, widely recognized in both scholarly literature and international standards:

Tone at the Top (Leadership Commitment) - Senior management must actively champion compliance and ethical conduct, signalling that integrity is a strategic priority (Kaptein, 2015). Leadership's behaviour sets the cultural tone for the organization.

Code of Conduct and Policies - A well-structured code of conduct articulates expected behaviours, ethical values, and legal obligations. It serves as both a guiding document and a reference point for decision-making (Parker, 2022).

Risk-Based Controls - Controls should be proportionate to the level of risk — allocating resources where exposure is greatest. For example, enhanced due diligence for politically exposed persons (PEPs) or high-value transactions (FATF, 2022).

Internal Reporting Mechanisms and Whistleblower Protection - Safe and confidential channels for reporting misconduct are critical for detecting risks early. The EU Whistleblower Directive (2019/1937) and Ukraine's 2020 whistleblower legislation both underscore the importance of retaliation protection (European Commission, 2023).

Integrating Compliance into Corporate Culture

Scholars consistently warn against treating compliance as a mere "box-ticking exercise" that satisfies external regulators but fails to influence organizational behaviour (Kaptein, 2015). Instead, compliance must become culturalized — woven into the values, incentives, and daily practices of the organisation.

Kaptein's (2008) *Corporate Ethical Virtues Model* suggests that ethical organizational culture consists of clarity (clear expectations), congruency (leaders as role models), feasibility (resources to act ethically), supportability (peer support), and sanction ability (rewarding compliance and sanctioning misconduct). When these cultural attributes are present, compliance programs are more likely to be internalized by employees and less likely to exist merely on paper.

Case in Point. Siemens Compliance Overhaul. *Following its €1.6 billion bribery settlement in 2008, Siemens implemented one of the most comprehensive compliance programs in the world, including a global compliance organization, real-time transaction monitoring, and mandatory training for over 300,000 employees. The program became a benchmark for multinational corporations, demonstrating that a*

well-designed compliance function can restore trust and create competitive advantage (Weismann, 2009).

Implications for Practice:

- For organizations - especially those operating in jurisdictions with rapidly evolving regulatory frameworks such as Ukraine - robust compliance programs provide:
- Regulatory Shield - Demonstrating “adequate procedures” can reduce liability in enforcement actions.
- Operational Efficiency - Risk-based controls prevent costly disruptions from fines, litigation, or reputational crises.
- Investor Confidence - Transparent compliance programs attract investors and improve credit ratings.
- Cultural Resilience - Embedding compliance into organizational culture fosters employee trust and ethical decision-making.

3.6 Comparative Analysis: EU vs. Ukrainian Standards

The comparative analysis of EU and Ukrainian compliance frameworks highlights both convergence and divergence in regulatory approaches (table 3.1). While the EU offers a highly institutionalized and mature compliance regime, Ukraine is in a period of rapid reform, seeking to harmonize its legal landscape with European standards as part of its EU accession agenda (European Commission, 2023).

Table 3.1 Key Areas of Comparison

Aspect	European Union (EU)	Ukraine
Data Protection	General Data Protection Regulation (GDPR) is one of the most comprehensive data protection regimes globally, guaranteeing data subject rights, requiring lawful processing, and imposing significant penalties for violations (European Commission, 2018).	Ukraine’s Personal Data Protection Law is under revision to achieve GDPR equivalence. Current enforcement remains limited but reform is ongoing, supported by EU technical assistance (UNDP Ukraine, 2023).
Anti-Corruption	EU anti-corruption efforts rely on a combination of directives (e.g., anti-money laundering directives) and national implementations. Institutions like OLAF and EPPO investigate cross-border corruption and fraud (OECD, 2023).	Ukraine has specialized institutions: NABU (investigation), SAPO (prosecution), and HACC (adjudication), which have significantly improved enforcement against high-level corruption since 2019 (Council of Europe, 2021).

Whistleblower Protection	Directive (EU) 2019/1937 mandates internal and external reporting channels and prohibits retaliation against whistleblowers (European Commission, 2023).	Ukraine adopted a whistleblower protection law in 2020, offering confidentiality and rewards for reporting corruption. Implementation is still maturing, and cultural barriers to reporting remain (Transparency International Ukraine, 2023).
Enforcement Capacity	Strong supervisory authorities (e.g., national data protection authorities, financial intelligence units) with sanctioning powers and EU-level coordination (EDPB, EPPO) (European Data Protection Board [EDPB], 2023).	Enforcement capacity is growing but uneven. Judicial independence reforms and institutional strengthening continue, with international oversight helping to maintain momentum (OECD, 2022).

From a regulatory theory perspective, the EU operates within what Baldwin, Cave, and Lodge (2012) describe as a "mature regulatory state," where rules are deeply institutionalized, enforcement is consistent, and there is a strong tradition of judicial oversight. The GDPR's extraterritorial reach exemplifies the EU's ambition to act as a global regulatory power (Bradford, 2020).

Ukraine, conversely, is in what might be called a transitional compliance phase — building institutions, passing new laws, and gradually increasing enforcement credibility. While significant progress has been made (e.g., NABU and HACC), challenges remain in ensuring independence, consistency, and public trust in enforcement outcomes (Council of Europe, 2021).

3.7 Emerging Trends and Future Challenges

The compliance landscape is increasingly dynamic, shaped by technological innovation, societal expectations, and geopolitical developments. For both EU and Ukrainian organizations, the coming decade will require not only adherence to existing laws but also anticipation of regulatory trends and the capacity to adapt to new compliance frontiers.

AI and Compliance

The introduction of the EU Artificial Intelligence Act (AI Act) marks a watershed moment in global technology regulation. The AI Act adopts a risk-based framework, classifying AI systems into categories ranging from minimal risk to "unacceptable risk," with strict obligations for high-risk systems (European Commission, 2024). Organizations deploying AI for critical infrastructure, employment screening, or biomet-

ric identification will be required to implement:

> Robust data governance to ensure training data quality and prevent bias.

> Human oversight mechanisms to guarantee accountability in decision-making.

> Transparency and documentation obligations to facilitate regulatory audits.

From a compliance perspective, AI governance will require organizations to expand their risk management frameworks to address algorithmic accountability and ethics-by-design principles (Brundage et al., 2020). Ukraine, as part of its EU accession process, is expected to gradually align with the AI Act, creating compliance obligations for domestic AI developers and users.

ESG Regulations and Corporate Sustainability

Environmental, Social, and Governance (ESG) considerations have moved from voluntary disclosure to mandatory reporting requirements. The EU Corporate Sustainability Reporting Directive (CSRD) requires large companies and listed SMEs to disclose sustainability information, including carbon emissions, diversity metrics, and supply chain due diligence (European Parliament, 2022).

This shift reflects what Parker (2022) calls “compliance beyond compliance,” where companies are judged not only by their adherence to minimum legal requirements but also by their contribution to societal goals. For Ukrainian companies seeking access to EU capital markets or partnerships, adopting ESG reporting practices will be critical for maintaining competitiveness and investor trust.

Global Convergence of Compliance Standards

One of the most significant global trends in corporate governance and compliance is the gradual convergence of regulatory frameworks. Ukraine’s ongoing harmonization with European Union standards—particularly in the areas of data protection, competition law, and anti-corruption—is expected to reduce regulatory fragmentation and foster a more predictable and transparent business environment (European Commission, 2023). This alignment not only facilitates trade and investment but also enhances investor confidence by bringing Ukrainian regulatory practices closer to those of the EU single market.

At the same time, convergence presents several challenges that organizations and policymakers must address. First, the implementation of EU-equivalent compliance controls can create cost pressures for companies, particularly for small and medium-sized enterprises that may lack the resources for complex compliance infrastructures. Second, effective convergence depends on Ukraine’s ability to ensure that its supervisory authorities are well-resourced, independent, and capable of consistent enforcement. Finally, multinational corporations must manage overlapping obligations across multiple jurisdictions, including the EU, United States, and other markets, which necessitates the development of integrated, risk-based compliance strategies to avoid duplication and ensure coherence across global operations.

Geopolitical and Cybersecurity Risks

Emerging compliance challenges also stem from heightened geopolitical risk and cy-

bersecurity threats. Sanctions regimes, export controls, and supply chain security requirements are becoming more stringent, particularly in response to global conflicts and cyberattacks (OECD, 2023). Organizations must integrate geopolitical risk assessments into their compliance programs, a development that is especially relevant for Ukrainian businesses operating under wartime conditions.

Pedagogical Insight

For students, these trends highlight that compliance is no longer static but strategic and anticipatory. Compliance officers of the future will need to be proficient not just in law, but also in technology, sustainability metrics, and risk analytics. This multidisciplinary demand underscores the need for continuous professional education and the cultivation of an adaptive compliance culture.

Practical Exercises

The following exercises are designed to translate theoretical knowledge into practical competence. Students are expected to engage critically with real-world scenarios, apply relevant standards and laws, and produce deliverables that reflect professional compliance practice.

Exercise 1: Compliance Mapping

Learning Objective: To develop the ability to identify, categorize, and present key compliance obligations applicable to an organization operating in both EU and Ukrainian jurisdictions.

Task Description: Students will prepare a compliance obligations chart for a selected company (e.g., technology firm, manufacturing enterprise, or financial institution) seeking to operate in both regulatory environments. The chart should cover at least three domains:

> Data Protection: GDPR and Ukraine's Personal Data Protection Law.
> Anti-Corruption: EU Anti-Money Laundering Directives (AMLD 4–6), NABU and HACC enforcement.
> Transparency and Reporting: Corporate disclosures, ESG obligations (CSRD), and Ukrainian financial reporting standards.

A structured one-page compliance mapping table including: Legal/regulatory source. Key compliance requirements. Responsible function or department. Implementation timeline or reporting cycle.

Evaluation Criteria: Accuracy and comprehensiveness of identified obligations. Clarity of presentation and logical organization. Practical relevance for corporate compliance teams

Exercise 2: GDPR Breach Response Simulation

Learning Objective: To simulate organizational response to a significant data breach, practicing compliance with GDPR timelines and communication requirements.

Task Description: Students will be divided into teams representing: Chief Compliance Officer, IT Security Lead, Legal Counsel, Communications Officer, Senior Management Representative

The team will respond to a simulated incident in which personal data of 50,000 EU customers has been compromised. The response plan must address: Incident containment and technical investigation. Notification to supervisory authority within 72 hours (Art. 33 GDPR). Notification to data subjects where required (Art. 34 GDPR). Documentation of mitigation and corrective measures

Deliverable: A concise incident response strategy (5–10 minutes presentation or two-page written report) including timeline, roles, and key actions.

Evaluation Criteria: Alignment with GDPR obligations and deadlines. Clear delineation of responsibilities and decision-making process. Quality, coherence, and realism of the proposed plan.

Exercise 3: Compliance Risk Matrix Development

Learning Objective: To build a compliance risk assessment tool that prioritizes risks according to likelihood and potential impact, forming the basis for mitigation strategies.

Task Description: Using a case study of a mid-sized energy company, students will: Identify at least five compliance risks (e.g., environmental violations, anti-bribery exposure, workplace safety breaches, data privacy incidents). Assess each risk based on likelihood (low/medium/high) and impact (low/medium/high). Visualize results in a risk matrix (2x2 or 3x3 grid). Propose targeted mitigation strategies for the two highest-priority risks.

Deliverable: A risk matrix accompanied by a brief explanatory narrative (max. one page).

Evaluation Criteria: Appropriate and realistic identification of risks. Sound prioritization logic based on likelihood and impact. Practicality and effectiveness of proposed mitigation measures

Notes: These exercises are deliberately structured to require cross-functional thinking, mirroring the complexity of real compliance work. Students are encouraged to reference ISO 37301:2021, GDPR, and Ukrainian legal frameworks when designing solutions. The outcome should demonstrate not only regulatory knowledge but also the ability to operationalize compliance principles in a business context.

Target Questions

1. Why is compliance a strategic function, not just a legal necessity?
2. What are the key differences between EU and Ukrainian anti-corruption enforcement mechanisms?
3. How can ISO 37301 improve organizational resilience?

References for Self-Study

1. Australian Securities and Investments Commission. (2023). *Annual enforcement report.* https://asic.gov.au
2. Baldwin, R., Cave, M., & Lodge, M. (2012). *Understanding regulation: Theory, strategy, and practice* (2nd ed.). Oxford University Press.
3. Bradford, A. (2020). *The Brussels effect: How the European Union rules the world.* Oxford University Press.
4. Braithwaite, J. (2011). The essence of responsive regulation. *UBC Law Review, 44*(3), 475–520.
5. Coates, J. C. (2007). The goals and promise of the Sarbanes–Oxley Act. *Journal of Economic Perspectives, 21*(1), 91–116. https://doi.org/10.1257/jep.21.1.91
6. Coffee, J. C. (2020). *Corporate governance and compliance: What works and what doesn't.* Oxford University Press.
7. Council of Europe. (2021). *Anti-corruption reforms in Ukraine.* https://www.coe.int
8. European Commission. (2018). *General Data Protection Regulation (GDPR).* https://gdpr.eu
9. European Commission. (2023). *Whistleblower protection directive – implementation guidance.* https://commission.europa.eu
10. European Commission. (2024). *Artificial Intelligence Act proposal.* https://digital-strategy.ec.europa.eu
11. European Data Protection Board. (2022). *Annual overview of GDPR enforcement and fines.* https://edpb.europa.eu
12. European Data Protection Board. (2023). *Meta Ireland decision.* https://edpb.europa.eu
13. European Parliament. (2022). *Corporate Sustainability Reporting Directive (CSRD).* https://www.europarl.europa.eu
14. European Securities and Markets Authority. (2023). *MiFID II framework overview.* https://www.esma.europa.eu
15. Financial Action Task Force. (2022). *International standards on combating money laundering and the financing of terrorism & proliferation.* https://www.fatf-gafi.org
16. Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and organizations: Software of the mind* (3rd ed.). McGraw-Hill.
17. International Labour Organization. (2022). *International labour standards on decent work.* https://www.ilo.org
18. International Monetary Fund. (2023). *World economic outlook: Global fiscal frameworks.* https://www.imf.org
19. International Organization for Standardization. (2021). *ISO 37301:2021 Compliance management systems — Requirements with guidance for use.* https://www.iso.org

20. Kaptein, M. (2008). Developing and testing a measure for the ethical culture of organizations: The corporate ethical virtues model. *Journal of Organizational Behavior, 29*(7), 923–947. https://doi.org/10.1002/job.520

21. Kaptein, M. (2015). The effectiveness of ethics programs: The role of scope, composition, and sequence. *Journal of Business Ethics, 132*(2), 415–431. https://doi.org/10.1007/s10551-014-2296-3

22. KPMG. (2022). *Corporate compliance and ISO 37301 adoption in Europe.* https://home.kpmg

23. National Anti-Corruption Bureau of Ukraine. (2022). *Annual report.* https://nabu.gov.ua

24. North, D. C. (1990). *Institutions, institutional change, and economic performance.* Cambridge University Press.

25. OECD. (2022). *Corporate governance of state-owned enterprises in Ukraine: Review and recommendations.* https://www.oecd.org

26. OECD. (2023). *OECD guidelines for multinational enterprises on responsible business conduct.* https://mneguidelines.oecd.org

27. Parker, C. (2022). *The open corporation: Effective self-regulation and democracy* (2nd ed.). Cambridge University Press.

28. Personal Data Protection Commission. (2023). *Enforcement decisions and statistics.* https://www.pdpc.gov.sg

29. Schaffer, R., Agusti, F., & Dhooge, L. (2021). *International business law and its environment* (11th ed.). Cengage Learning.

30. Spalding, A. (2011). The ironies of international bribery law. *UCLA Law Review, 55*, 783–852.

31. Transparency International Ukraine. (2023). *Compliance trends in Ukrainian business.* https://ti-ukraine.org

32. United Nations Development Programme Ukraine. (2023). *Support to data protection reform.* https://www.undp.org/ukraine

33. United Nations Office on Drugs and Crime. (2019). *United Nations convention against corruption: Legislative guide for the implementation of the United Nations convention against corruption.* https://www.unodc.org

34. U.S. Department of Health & Human Services. (2023). *Summary of the HIPAA privacy and security rules.* https://www.hhs.gov

35. U.S. Department of Justice. (2023). *FCPA enforcement statistics and policy updates.* https://www.justice.gov

36. Vogel, D. (2018). *The politics of precaution: Regulating health, safety, and environmental risks in Europe and the United States.* Princeton University Press.

37. Weismann, M. F. (2009). The foreign corrupt practices act: The failure of the self-regulatory model of corporate governance in the global business environ-

ment. *Journal of Business Ethics, 88*(4), 615–661. https://doi.org/10.1007/s10551-009-0317-8

38. World Bank. (2023). *Doing business in East Asia and the Pacific: Regulatory overview.* https://www.worldbank.org
39. World Trade Organization. (2022). *World trade report 2022.* https://www.wto.org
40. Zhang, L. (2022). China's evolving cybersecurity and data protection framework: Implications for global business. *Journal of International Business Policy, 5*(3), 402–420. https://doi.org/10.1057/s42214-022-00128-3

Assignments for Self-Study

1. *Essay (2–3 pages).* Compare GDPR and Ukraine's Personal Data Protection Law. Discuss challenges Ukrainian companies face when working with EU partners.
2. *Research Task.* Analyse a recent NABU case and evaluate its compliance implications.
3. *Presentation.* Design a compliance program for a hypothetical tech company expanding to the EU market.

Chapter 4. Compliance Management Systems: Elements and Functions

Learning Outcomes

After studying this chapter, learners will be able to:

- Operate with knowledge of tools for constructing and managing a compliance system, including internal policies, codes of ethics, and audit mechanisms.
- Form a culture of ethical conduct in the organization.
- Demonstrate autonomy in planning and performing tasks related to managing the compliance system.

***Key words*:** compliance policy, compliance system, compliance standards, ethics, code of ethics and conduct, principle of "Tone at the Top", control, reporting and response

Main Definitions

A compliance system is a set of policies, procedures, roles, control mechanisms, and communications aimed at ensuring that compliance of an organization's activities with the requirements of legislation, international standards, internal regulations, and ethical norms.

A compliance policy is a document adopted by the company's management that defines the basic principles and requirements for compliance programs in an organization, containing rules and procedures that must be followed to ensure compliance of the company's activities with regulatory and legal acts and international standards.

The principle of «Tone at the Top» is a management principle that describes how the behavior, values, and communication of the company's management shape the overall ethical atmosphere in the organization. It assumes that top management sets the standards for transparency, accountability, and compliance, which are then transmitted to all levels of the corporate culture.

Standards, Laws, and Regulations

ISO 37301:2021 "Compliance management systems", Law of Ukraine "On Prevention of Corruption" dated 14.10.2014 № 1700-VII, Methodological recommendations on the application of tools and mechanisms for the transformation of various spheres of functioning of higher education institutions on the principles of transparency and integrity, approved by Order of the Ministry of Education and Science of Ukraine dated 17.04.2025 № 576

List of subsections

4.1 Theoretical Foundations and Scientific Approaches to Compliance System Formation

4.2 Strategic foundations of compliance: policies, ethics, reputation.

4.3 Compliance operating system: roles, processes, control.

4.4 Monitoring, reporting and response.

4.5 Compliance as the Foundation of Corporate Ethics and Sustainability

4.1 Theoretical Foundations and Scientific Approaches to Compliance System Formation

In the modern business environment compliance ceases to be just a tool of legal protection, but is transformed into the foundation of ethical, transparent and responsible corporate conduct. Compliance policy, compliance standards and ethics form the triune foundation on which trust is built among company, its employees, partners and society. Each of these elements has its own nature.

The issue of forming a compliance system at an enterprise, institution, orgnization, including taking into account strategic, operational and control aspects, was studied by such authors as Ovsienko O., Svitlychnyi O., Shvydka T., Khaletska K., Bortnikova M., Stasyuk N., Malinovska Yu. and others.

In particular, Ovsienko O. in co-authorship with Svitlychny O. examines the prospects for the development of compliance consulting in Ukraine, focusing on the role of ethics, anti-corruption policy and adaptation of international requirements to the national context. Shvydka T. and Khaletska K. analyze compliance control in the corporate governance system, paying attention to the roles of the compliance officer, management, internal audit and monitoring mechanisms. Bortnikova M., Stasyuk N. and Malinovska Y. investigate the applied tools of compliance, in particular methods of personnel involvement, training, communication and the emotional component as factors in the formation of an ethical culture.

The generalization of scientific approaches indicates the gradual formation of a national compliance model that combines strategic vision, operational flexibility and control transparency, meeting both local risks and global standards of responsibility.

4.2. Strategic foundations of compliance: policies, ethics, reputation

A compliance policy is a document adopted by the company's management that defines the basic principles and requirements for compliance programs in an organization. It contains rules and procedures that must be followed to ensure compliance of the company's activities with regulatory acts and international standards (Business, 2021).

In the field of corporate governance, the concepts of *compliance policy, compliance standards* and *ethics* form the triune foundation of responsible activity. Although these terms are often used together, each has a unique meaning, function, and source of origin. For the better understanding of their role in constructing an effective compliance

system, it is advisable to compare them according to the key criteria: content, function, source, and example of application (Table 4.1).

Table 4.1 The essence and interrelationship of concepts in the corporate compliance system

Concept	Definition	Function in compliance	Source / reference	Application example
Compliance Policy	An internal company document regulating the rules of conduct, processes	Formalizes requirements, ensures control and compliance	Internal regulations, ISO 37301	Anti-corruption policy, privacy policy
Compliance standards	External regulatory acts, international or national requirements	Serve as the basis for policy development, set the framework	GDPR , FCPA , ISO, labor legislation	Data protection, labor rights, anti-corruption requirements
Ethics	A system of moral principles that determines what is good and fair	Forms values, influences corporate culture	Philosophy, professional codes, ISO 26000	Code of Ethics, Principles of Non-Dis-crimination, respect

Thus, compliance standards form external requirements that define the framework of responsible corporate behavior, while compliance policies adapt these requirements to the internal environment of the company, taking into account its structure, culture and operational processes. Ethics, in turn, determines not only the legal correctness of such policies, but also their moral validity, fairness to all participants in the interaction. For example, GDPR requirements for the protection of personal data encourage a company to develop a privacy policy, and ethical principles ensure that this policy is not a formal declaration, but truly protects the rights of users and demonstrates respect for their privacy .

Compliance policies must meet international requirements, as they define generally accepted standards of transparency, legal compliance, and ethical behavior in the global business environment. Compliance with requirements such as GDPR, ISO 37301, FCPA, UK Bribery Act allows a company to create internal regulations that are not only consistent with the law, but also reflect the principles of fairness, respect for human rights and social responsibility. Although the FCPA (US) and the UK Bribery Act (Great Britain) are not mandatory for most Ukrainian enterprises, their provisions can

serve as a guideline in the development of anti-corruption policies. In particular, the extraterritorial nature of these acts is important for companies that have or plan to have international relations, investments or contracts with foreign partners. This approach helps to reduce legal risks, increase trust from customers, partners and regulators, and also forms the company's reputation as a reliable and ethically mature market participant.

Adapting global compliance policies to the local context is not just a matter of translating documents, but a process of aligning values, norms, and practices that requires a deep understanding of international standards, sensitivity to cultural differences, and the ability to transform formal requirements into a living, effective system that works in a real environment. Below are the summarized steps of this process — as a guide for companies seeking to combine global ethics with local reality (Table 4.2).

Table 4.2 Stages of adapting global compliance policies to the local context

Stages	Content	Application context
1. Analysis of global requirements	Study of international standards, regulatory norms, industry codes	For example: GDPR , ISO 37301, FCPA / UK Bribery Act, anti-corruption directives
2. Assessment of the local environment	Analysis of national legislation, cultural features, business practices	Considering legal risks, mental barriers and local expectations
3. Identifying points of conflict and agreeing	Identifying discrepancies between global norms and local realities	For example, different approaches to data protection or corporate ethics
4. Adaptation of formulations and procedures	Translation of policies into local language, adaptation of terminology, clarification of procedures	It is important to keep the essence, but make it understandable for local workers
5. Involvement of local stakeholders	Consultations with local lawyers, HR, and heads of departments	This increases policy acceptance and effectiveness.
6. Training and communication	Conducting trainings, explaining changes, creating local guidelines	Creating a compliance culture through clear language and examples
7. Monitoring and correction	Implementation of feedback mechanisms, regular audit of adapted policies	Flexibility and continuous improvement are the key to efficiency

In today's business environment, compliance policies are no longer a formality - they are becoming a strategic management tool that affects the reputation, trust and long-term sustainability of the company. Ethical principles embedded in corporate policies not only regulate the behavior of employees, but also shape the company's image in the eyes of partners, customers and investors. At the same time, the strategic goals of the enterprise - sustainable development, transparency, innovation - cannot be implemented without a clear compliance system. The following is a summarized table that demonstrates this relationship in a structured form (Table 4.3).

Table 4.3 The impact of compliance policies on the strategic goals and reputation of the enterprise

Component	Impact on strategic goals	Impact on reputation
Code of Ethics and Conduct	Forms the basis of a corporate culture that supports the goals of sustainable development, transparency and responsibility	Promotes trust from customers, partners, investors; demonstrates company values
Compliance policies	Ensure compliance with legislation, reduce risks, support strategic stability	Show that the company acts honestly, predictably, and is responsible for its actions
Anti-corruption and antitrust policies	Increase competitiveness, open access to international markets	Protect the company from scandals, legal sanctions, and loss of trust
Internal control and reporting mechanisms	Support strategic risk management, ensure process efficiency	Demonstrate transparency and a willingness to self-monitor, which strengthens the reputation
Compliance training and communication	Create a culture of awareness that supports strategic change and innovation	Create an image of the company as a responsible employer who cares about ethics

Implementing effective compliance policies not only helps an organization achieve its strategic goals, but also builds its reputation as a responsible, transparent, and ethically mature market entity. However, no policy will be effective without internal support, primarily from management. Especially leaders who set the tone for corporate culture, define the boundaries of what is acceptable, and set an example for others to follow. In this context, the key principle is the "Tone at the Top", which describes how management behavior and values shape the ethical climate in the company. The following is a summarized table revealing the main components of this principle (Table 4.4).

Table 4.4 The content of the principle "Tone at the Top"

Component	Content	Impact on the organization	Example of manifestation
Leadership values	Personal beliefs, ethical standards demonstrated by top management	Form the basis of corporate culture	The management of JSC CB "PrivatBank" publicly supports the policy of transparency, ethics and prevention of conflicts of interest
Personal behavior	Actions, decisions, reactions of managers in daily practice	Become a benchmark for employees, influence trust	Microsoft CEO Satya Nadella actively promotes a culture of inclusion, ethics, and responsibility
Communi-cation of values	How management talks about ethics, compliance, transparency	Sets priorities, creates an atmosphere of openness	Patagonia founders openly communicate about ethical principles, sustainability, and social responsibility
Maintaining control mechanisms	Real participation in the implementation of compliance procedures	Increases system efficiency, reduces risks	Ukrainian communities implement anti-corruption compliance with the support of local government leaders
Responding to violations	How managers respond to ethical violations or complaints	Determines the level of trust and fairness	Fid Foundation develops training for leaders who respond to violations through transparent mechanisms

4.3 Compliance Operating System: Roles, Processes, Control

The key elements of a robust compliance operating system, their defining characteristics, and practical implementation examples are summarized in the table below. This breakdown highlights the shift from formal documentation to an integrated ethical culture (Table 4.5).

Table 4.5 Compliance operating system Elements: roles, processes, control

Element	Characteristics	Company example
Policies and procedures	Documents should not be formal, but adapted to the real risks and culture of the company. They should be clear, accessible and regularly updated.	JSC CB “PrivatBank” implements policies on conflict of interest, data protection and anti-corruption
Roles and responsibilities	Clear separation of functions, namely, the compliance officer coordinates, management sets the tone, and employees follow the policies.	Company Microsoft has an independent compliance function, accountable to the supervisory board
Training and communication	Constantly informing employees about policies, risks, ethical standards. Creating a culture of awareness.	Fid Foundation conducts trainings for businesses and communities
Methods of staff engagement	Employees should not just be informed, but actively involved through surveys, cases, and internal initiatives.	Patagonia involves staff in environmental and ethical initiatives
Development of training programs	Programs should be adapted to roles, include motivational elements, examples and interactive formats.	Nova Poshta LLC implements internal courses on ethics and responsibility
Emotional component	Trust, openness, support are key elements that influence behavior. Compliance should be a culture, not a fear.	UNIC promotes ethical business culture through dialogue, cases, and support for whistleblowers

A summary of the key roles within the compliance framework, their core responsibilities, and relevant industry examples is presented below. This classification highlights the collaborative nature of maintaining an ethical and legally compliant business environment (Table 4.6).

Table 4.6 Roles and Responsibilities in Compliance

Role in compliance	Responsibility
Compliance Officer	- development and implementation of compliance programs; - internal investigations; - risk monitoring.

Company management	- policy approval; - resource provision; - support of a culture of ethics and transparency.
Directors	- AML/CTF, sanctions, data protection; - regional compliance officers; - interaction with regulators
HR / Staff training	- conducting annual compliance training; - integrating ethical standards into corporate culture.
Legal Department	- contract review; - identification of legal risks; - implementation KYC/Due Diligence.

4.4. Monitoring, Reporting and Response: System Protection

A compliance operating system forms the ethical framework of the enterprise through policies, codes of conduct, training and reporting mechanisms, but for its effective functioning it is necessary to implement an internal control system that ensures the practical implementation of these principles. Such control includes risk assessment, development of control procedures, integration into business processes and ongoing monitoring, creating mechanisms for detecting, preventing and correcting violations (Table 4.7).

Table 4.7 Implementation of internal control systems for compliance management

System component	Function description and meaning	Implementation example
Control environment	Formation of ethical culture, policies, standards of conduct	JSC «Ukreximbank» - internal control policy integrated into corporate governance
Risk assessment	Identification and analysis of compliance risks (sanctions, corruption, conflict of interest)	LIGA360 — a tool for assessing counterparty risks and sanctions background
Control measures	Procedures for verification, reporting, registration of gifts, and conduct of counterparties	Manufacturing enterprises - implementation of local control procedures

Information systems	Collection, analysis and transmission of data on compliance incidents, risks	LIGA360, YouControl — automated systems for AML / KYC , Due Diligence
Monitoring and auditing	Verification of ystem effectiveness, internal audit, adjustments	Banks, insurance companies — mandatory internal audit according to the NBU

The most common international concept is COSO, which covers all five components of internal control. It allows not only to prevent violations, but also to form a culture of responsibility and transparency (LigaZakon, 2023).

A summary of the core compliance control mechanisms, their functional significance, and practical implementation cases is presented in the table below. These tools form the basis of a proactive approach to risk management and corporate governance (Table 4.8).

Table 4.8 Compliance control mechanisms

Control mechanism	Function description and meaning	Implementation example
Compliance audit	Systematic verification of compliance of policies, procedures, and actions with legal and ethical requirements.	JSC “Sense Bank” implemented a compliance control department and reputation risk audit
Risk monitoring	Constant monitoring of the behavior of employees, counterparties, and financial transactions.	PJSC “ARCELORMITTAL KRYVYI RIH” carries out monitoring environmental and social risks
Internal audits	Regular local audits of processes, reporting, gift registration, and conflicts of interest.	JSC “Ukreximbank” conducts internal audits in accordance with the control policy

Compliance reporting is a key element of the internal control and transparency system. It is compiled in cases where the company conducts an audit of policies, records conflicts of interest, responds to violations, carries out staff training or monitors risks. Such reporting can be internal - for management, the supervisory board or the compliance department, or external - for regulators, shareholders and partners. Reports are often published on the official websites of companies in the sections “Corporate Governance”, “Sustainability” or “Ethics and Responsibility”, especially if the company seeks to demonstrate openness and compliance with international standards. In public companies, such reporting can also be part of non-financial reporting or ESG documents (Table 4.9).

Table 4.9 Compliance reporting

Reporting type	Purpose	Company example
Internal audit report	Verification of compliance of policies, procedures, actions with legal and ethical requirements	YouControl conducts regular compliance audits in B2B services
Conflict of Interest Report	Recording and analyzing situations where personal interests may influence decisions	JSC CB PrivatBank has a conflict of interest policy that includes reporting
Staff training report	Displaying the scope, topics and results of compliance trainings	LLC Nova Poshta implements internal courses on ethics and responsibility
Incident/ Violation Report	Registration of cases of policy violations, including whistleblower actions	UNIC supports a culture of reporting violations through ethical channels
Risk monitoring report	Analysis of the behavior of employees, counterparties, financial transactions	LIGA ZAKON uses digital tools for sanctions monitoring and KYC
Tax Compliance Report	Displaying compliance with tax regulations, voluntary compliance	JSC “Ukreximbank” integrated internal control policy into corporate governance

4.5. Compliance as the Foundation of Corporate Ethics and Sustainability

Thus, the compliance system is not a set of formal documents, but a living ethical architecture that permeates all levels of corporate governance. Its effectiveness depends on the harmonious interaction of external standards, internal policies and moral principles that form a culture of responsibility. As company cases show – from PrivatBank to Microsoft, from YouControl to Patagonia – successful implementation of compliance is possible only if it is not perceived as an obligation, but as a value. Internal control, training, emotional openness and a clear delineation of roles are not only technical components, but also manifestations of a deeper desire for justice. In a global context, compliance becomes a language of trust, and in a local context - a tool for transforming business into an ethical community. That is why

its development is not only a legal task, but also a moral responsibility of each organization.

Practical Exercises

Exercise 1 - Digital Transformation of Ethics

Background: EQS Group faced challenges in managing ethical violations and conflicts of interest across multiple European branches. Traditional reporting mechanisms lacked transparency and failed to protect whistleblowers effectively.

Task: Imagine you are a Compliance Officer at a multinational firm.

1. List three primary risks of using «traditional» (non-digital) reporting channels.

2. Explain how an anonymous digital platform changes the «Tone at the Top» and employee trust.

3. Discussion: Does technology alone create a culture of responsibility, or does it require additional human intervention?

Exercise 2 - Balancing Regulation and Agility

Background: Small businesses often view excessive regulation as a burden rather than a benefit, leading to resistance and «formal» (fake) compliance. The European Commission proposed the «Smart Enforcement» concept to bridge this gap.

Task:

1 Define the «Smart Enforcement» concept based on the text.

2. Propose three specific ways a regulator can use «dialogue and adaptation» instead of just penalties.

Exercise 3 - ESG Integration in Heavy Industry

Background: As a major metallurgical producer, PJSC ArcelorMittal Kryvyi Rih (Ukraine) needed to manage a complex mix of environmental, social, and anti-corruption risks to maintain its international reputation.

Task:

1. Identify the three pillars of ESG (Environmental, Social, and Governance) mentioned in the text.

2. Analyze why an anti-corruption policy is essential for a company's Environmental strategy.

3. Strategy Session: Develop a brief outline for an «Internal Audit» focused on social risks (e.g., labor rights or community relations) for a large industrial plant.

Target Questions

1. What is a compliance policy?
2. What is the purpose of the compliance policy?
3. What do compliance standards include?
4. What is ethics in the context of compliance?
5. What role does a code of ethics and conduct play?
6. What is the impact of anti-corruption and antitrust policies?
7. What do internal control and reporting mechanisms provide?
8. What does the “Tone at the Top” principle describe?
9. What is a compliance audit?
10. What does risk monitoring in a compliance system include?

References for self-study

ISO 37301:2021 “Compliance management systems” (2021). URL: https://surl.li/sl-ghzg

1. Law of Ukraine “On Prevention of Corruption” dated 14.10.2014. № 1700-VII . URL : https://zakon.rada.gov.ua/laws/show/1700-18#Text
2. Methodological recommendations on the use of tools and mechanisms for the transformation of various spheres of functioning of higher education institutions on the principles of transparency and integrity, approved by Order of the Ministry of Education and Science of Ukraine dated 17.04.2025 № 576. URL: https://surl.li/ugcccr
3. Ovsiienko, O.V., & Svitlychnyi, O.S. (2021). Compliance consulting and prospects for its development in Ukraine. *Ekonomichna teoriia ta pravo*, 2 (45), 68-80. DOI: 10.31359/2411-5584-2021-45-2-68 [in Ukrainian].
4. Bortnikova, M.H., Stasiuk, N.R., & Malynovska, Yu.B. (2023). Formation of applied compliance tools at domestic enterprises. *Menedzhment ta pidpryiemnytstvo v Ukraini: etapy stanovlennia ta problemy rozvytku*, 1 (9), 125-134. URL: https://surl.li/kjuygw [in Ukrainian].
5. Shvydka, T., & Khaletska, K. (2020). Compliance control in the corporate governance system of business companies. *Hospodarske pravo i protsess*, 12, 88-94. DOI: 10.32849/2663-5313/2020.12.14 [in Ukrainian].
6. Company compliance policy: what should it include? (n.d.). *Protocol.* https://surl.li/vtrvdn [in Ukrainian].
7. Compliance: basic principles and significance in business. (n.d.). *LIGA:ZAKON.* https://surl.li/klcoxm [in Ukrainian].

8. How to achieve GDPR Compliance 2025: requirements and actions for business in Ukraine. (n.d.). *IT-Lawyer.* https://surl.lu/xzjgor [in Ukrainian].

9. Lomzhets, Yu., Halai, A., Derkach, S., & Datsko, K. (n.d.). *Analytical study «The role of a leader in combating corruption: an analytical review of the implementation of the «Tone At The Top» concept».* NAZK. https://surl.li/nyywcr [in Ukrainian].

10. Korshun, A. (n.d.). Compliance check: what is needed to implement an effective compliance model in a company. https://surl.lt/mtvtme [in Ukrainian].

11. Otsokolich, V. (n.d.). TOP-10 components of an effective compliance system. *Blog IFI.* https://surl.li/aouyai [in Ukrainian].

12. Amirian, D. (n.d.). Compliance and ethical culture of the company. *SAYENKO KHARENKO.* https://surl.li/jytetq [in Ukrainian].

13. Everything you need to know about compliance. (n.d.). *YouControl.* https://you-control.com.ua/articles/vse%2C-shcho-neobkhidno-znaty-pro-komplaiens/ [in Ukrainian].

14. Otsokolich, V. (n.d.). Internal control as an element of the company's compliance system. *PWC Ukraine.* https://surl.lt/kqfynw [in Ukrainian].

15. Implementation of compliance at a manufacturing enterprise. Where to start? (n.d.). *LIGA:ZAKON.* https://surl.li/mnspbx [in Ukrainian].

16. Kurilov, Ye. (n.d.). Tax compliance and basic elements of compliance risk management: the vision of the OECD and the IMF. *Visnyk.Ofitsiino pro podatky.* https://surl.li/nbczwh [in Ukrainian].

17. Thomann, E., & Sager, F. (2017). Moving beyond legal compliance: innovative approaches to EU multilevel implementation. *Journal of European Public Policy*, 24 (9), 1253-1268. DOI: 10.1080/13501763.2017.1314541

18. PwC Global Compliance Survey. (2025). *Time to act faster: How to reboot compliance to accelerate processes and overcome obstacles.* PwC Ukraine. https://www.pwc.com/ua/uk/survey/2025/komplaiens-2025.html [in Ukrainian].

Assignments for Self-Study

1. Research a major corporate scandal in open sources (for example, a case related to corruption or a data privacy breach).

   Analyze how the lack of ethical leadership or a violation of the «Tone at the Top» principle contributed to the crisis.

   Identify which specific elements of the compliance system - such as policies, control mechanisms, or training - were missing or failed to function effectively in this instance.

2. Based on the theoretical foundations of the system, choose two compliance domains (e.g., Anti-corruption Compliance and Data Protection/GDPR). For each domain, briefly describe:

   Purpose: Why is this necessary for the organization?

   Typical Risks: What could go wrong (e.g., legal sanctions or loss of trust)?

   Compliance Measures: Which tools (audit, monitoring, training) help minimize these risks?

3. Create a simple conceptual map (mind map) that visualizes the relationships between the following elements mentioned in the chapter:

   The Triune Foundation: Compliance policy, standards, and ethics.

   Connecting Elements: The «Tone at the Top» principle and corporate culture.

   Outcome: The company's reputation and long-term strategic sustainability.

Chapter 5: Compliance Organizations, Corporate Culture & Leadership (CECO)

Learning Outcomes

After studying this chapter, learners will be able to:

- Explain the role and responsibilities of a Chief Ethics and Compliance Officer (CECO) within an organization's governance structure.
- Assess how corporate culture influences compliance effectiveness.
- Apply leadership approaches to foster an ethical and transparent business environment.

Key Words: compliance organization, corporate culture, CECO, ethics, leadership, tone at the top, organizational values.

Main Definitions

Compliance Organization – The structure, processes, and resources that ensure adherence to laws, regulations, internal policies, and ethical standards.

Corporate Culture – The shared values, beliefs, and behavioral norms within an organization that influence daily decision-making.

Chief Ethics and Compliance Officer (CECO) – A senior leader responsible for designing, implementing, and overseeing ethical and compliance programs.

Standards, Laws, and Regulations

1. International: ISO 37301 (Compliance Management Systems), ISO 37000 (Governance of Organizations), OECD Guidelines for Multinational Enterprises.

2. European Union: EU Whistleblowing Directive, Corporate Sustainability Reporting Directive (CSRD), EU General Data Protection Regulation (GDPR).

3. Ukraine: Law on Prevention of Corruption, Law on Personal Data Protection, Code of Ethics for Civil Servants.

List of Subchapters

5.1 The Role of the Compliance Organization in Corporate Governance

5.2 CECO: Functions, Authority, and Cross-Departmental Collaboration

5.3 Corporate Culture as a Foundation for Compliance Success

5.4 Leadership in Compliance: "Tone at the Top" and Leading by Example

5.1 The Role of the Compliance Organization in Corporate Governance

A compliance organization is the structural and functional part of a company responsible for ensuring that business operations align with applicable laws, regulations, industry standards, internal policies, and ethical norms. In corporate governance, the compliance function serves as a safeguard mechanism, ensuring that the organization's pursuit of profitability and growth does not conflict with its legal obligations or ethical responsibilities. In other words, compliance acts as a "guardian of integrity" – maintaining the delicate balance between business objectives and the rules that govern corporate behavior. This makes it a core element of modern governance systems, where trust and transparency are increasingly decisive factors for long-term success.

Historically, compliance was viewed as a "back-office" control task, primarily reactive in nature, focused on avoiding penalties and ensuring minimal legal conformity. Today, this perception has changed significantly. Modern governance frameworks (such as OECD Principles of Corporate Governance, EU directives, and national corporate codes) view compliance as an integrated strategic function that directly influences business resilience and competitiveness. Recent industry surveys confirm this shift: PwC's "Transformation 2025+" report highlights the evolution of compliance into a strategic value driver integrated into the business value chain.

Research by Treviño, Weaver, and Brown (2008) highlights that ethical leadership is essential for embedding compliance into the corporate culture. Leaders who demonstrate integrity in decision-making set behavioral norms that cascade throughout the organization, shaping how compliance policies are perceived and followed. Similarly, Kaptein (2015) emphasizes that effective compliance leadership involves integrating ethics and compliance principles into strategic planning, ensuring that these values influence core business decisions rather than being treated as isolated compliance checklists.

Recent studies also connect compliance effectiveness with the strength of corporate governance frameworks. Akinsola (2025) notes that strong governance structures, such as independent boards, clear accountability lines, and transparent reporting systems, significantly enhance the organization's ability to prevent misconduct and maintain regulatory alignment. This finding aligns with insights from the Diligent Blog (2024), which describes a clear correlation between robust governance practices and compliance maturity, particularly in complex regulatory environments.

In the Ukrainian context compliance functions in corporate governance are evolving under the influence of both EU regulatory alignment and heightened public expectations for corporate transparency. They stress that compliance units are increasingly involved in strategic discussions, crisis management, and stakeholder engagement.

An effective compliance organization contributes to governance in several ways:

Risk prevention and early detection – by systematically identifying potential legal, regulatory, or ethical risks before they escalate into major issues. For example, monitoring transactions to detect patterns that could indicate fraud or money laundering.

Value creation and reputation building – ethical conduct and adherence to rules foster credibility with customers, investors, and regulators. Research by Edelman Trust Barometer shows that companies with strong integrity cultures enjoy higher customer loyalty.

Operational continuity – compliance with safety, environmental, and data protection laws reduces the likelihood of disruptions caused by sanctions, lawsuits, or reputational crises.

Market access – in global trade, regulatory compliance is often a prerequisite for entering or remaining in specific markets (e.g., EU procurement rules or US Foreign Corrupt Practices Act requirements).

In this way, compliance transforms from a cost center into a value enabler, making governance more robust and future-proof.

The compliance organization performs a range of interconnected functions that together ensure the company operates within legal, regulatory, and ethical boundaries.

One of its core responsibilities is policy development and standard setting – this includes drafting and maintaining the Code of Conduct and a range of specific policies, such as those on anti-corruption, data protection, anti-harassment, environmental responsibility, and the prevention of conflicts of interest. These policies must not remain static; they are regularly updated to reflect evolving external regulations, especially in industries with strict oversight such as banking, pharmaceuticals, and energy.

An equally important role is monitoring, auditing, and control. This involves carrying out regular compliance audits and internal reviews to confirm that laws and internal policies are consistently followed. To support this, monitoring systems are established to detect violations, such as accepting gifts above permitted thresholds or mishandling personal data, before they escalate into serious risks.

In addition, the compliance function provides advisory and decision support to management. When ethical dilemmas or complex regulatory issues arise, compliance professionals act as trusted advisors, helping leadership choose lawful and ethical courses of action. They also ensure that major strategic initiatives, including mergers or new product launches, undergo compliance assessments before approval to identify and mitigate potential risks.

Finally, training and awareness-building ensure that policies are not only documented but also understood and applied in daily work. This includes organizing training programs for all levels of staff (from onboarding sessions for new hires to advanced workshops for managers) and embedding compliance into the company's culture through consistent communication, practical guidance, and role modelling by leaders.

The compliance function's position in the corporate hierarchy directly impacts its effectiveness. International best practice suggests that:

The compliance leader – whether titled Chief Ethics and Compliance Officer (CECO),

Compliance Manager, or another equivalent – should have direct access to the Board of Directors or Audit Committee.

The function must be independent from business units whose activities it monitors, to avoid conflicts of interest.

However, the Ukrainian reality differs. Many companies, particularly SMEs, do not have a formal compliance department. Instead, compliance tasks may be distributed among legal, HR, or internal audit teams. In such cases, corporate governance structures must clearly assign responsibilities and ensure decision-making independence for those performing compliance duties.

A growing trend in both the EU and Ukraine is the hybrid model, where compliance officers work closely with risk management, sustainability, and corporate social responsibility teams, integrating ethical and legal oversight into broader governance strategies.

In the European Union, compliance is embedded in governance frameworks due to strict laws such as:

EU Whistleblowing Directive (2019/1937) – requiring organizations with more than 50 employees to establish secure internal reporting channels.

General Data Protection Regulation (GDPR) – imposing strict personal data handling obligations.

Anti-Money Laundering Directives (AMLD) – setting due diligence obligations for financial transactions.

In Ukraine, compliance has developed fastest in:

Banking and finance – driven by National Bank regulations and international investor requirements.

Energy and extractive industries – due to transparency obligations under the Extractive Industries Transparency Initiative (EITI).

IT and outsourcing sectors – where compliance with EU GDPR is essential for working with European clients.

However, challenges remain, including insufficient awareness among top managers, limited training opportunities, and the perception of compliance as a “foreign” concept. Nevertheless, the ongoing EU integration process and post-war reconstruction plans are accelerating demand for compliance expertise.

5.2 CECO: Functions, Authority, and Cross-Departmental Collaboration

The Chief Ethics and Compliance Officer (CECO) is a senior executive responsible for developing, implementing, and overseeing an organization’s ethics and compliance program. The CECO ensures that business operations align with applicable laws, regulations, internal policies, and ethical standards. This role has become increasingly significant in a global business environment characterized by complex regulations, cross-border operations, and heightened public scrutiny.

In the EU, the role of CECO is linked to governance frameworks such as the OECD Guidelines for Multinational Enterprises and the EU Whistleblower Protection Directive (2019/1937), which require organizations to have internal reporting channels and responsible officers to manage them.

The CECO's role covers several core areas:

Strategic Leadership – Designing and promoting a long-term compliance strategy that integrates regulatory requirements, ethical principles, and internal controls into the organization's daily operations.

Policy Development and Standard Setting – Drafting and maintaining a Code of Conduct and specialized policies on anti-corruption, data protection, anti-harassment, environmental responsibility, and conflict-of-interest prevention, ensuring alignment with evolving regulations, especially in highly regulated industries such as banking, pharmaceuticals, and energy.

Monitoring, Auditing, and Control – Overseeing compliance monitoring programs, conducting internal audits and investigations, and implementing systems to detect violations (e.g., accepting prohibited gifts, mishandling personal data).

Advisory and Decision Support – Acting as a trusted advisor to senior management in resolving ethical dilemmas and assessing the compliance implications of strategic initiatives such as mergers, acquisitions, or new product launches.

Training and Awareness-Building – Organizing compliance training for all levels of staff, from onboarding sessions to specialized workshops for managers, and embedding compliance into the corporate culture through communication and role modeling.

Culture Building – Promoting a workplace environment that values transparency, accountability, and ethical decision-making, ensuring that compliance is seen not only as a legal requirement but as a core business value.

In this capacity, the CECO bridges the gap between regulation and business practice, safeguarding the organization's reputation, enhancing stakeholder trust, and ensuring long-term resilience.

In large European corporations, CECOs often operate with independence from the legal department, reporting directly to the board or audit committee to avoid conflicts of interest. For example, Siemens AG appointed a global CECO following its 2008 corruption scandal, with the officer empowered to halt business operations if compliance risks were identified.

In Ukraine, while the CECO role is not yet widespread, certain state-owned enterprises (e.g., Naftogaz, Ukrzaliznytsia) and private sector leaders in banking and IT have introduced similar positions, especially under the influence of international partners and corporate governance reforms.

Case in Point: CECOs in Action. *In 2024, Ericsson appointed Rebecca Rohr as Chief Compliance Officer after a period of U.S. Department of Justice monitorship due to a major bribery case. Her mandate includes driving cultural transformation, integrating investigative and compliance teams, and embedding ethical decision-making into daily business operations. Publication World Street Journal dated March 5, 2024 https://*

www.wsj.com/articles/ericsson-names-new-compliance-chief-07e455e0

ADM (Archer Daniels Midland) – Ben Bard, Chief Integrity Officer, oversaw global compliance, internal audit, and regulatory functions. His leadership was tested when the company faced U.S. Department of Justice and SEC investigations related to accounting practices, highlighting the CECO's role in high-stakes crisis management. Publication World Street Journal dated November 5, 2024 https://www.wsj.com/articles/adm-compliance-boss-to-depart-as-the-company-faces-accounting-problems-c2cb81c9

Scott E. Sullivan, Chief Integrity & Compliance Officer at Newmont Corporation, leads global programs on ethics, anti-corruption, internal investigations, and export controls, demonstrating how strong compliance leadership is vital in multinational, high-risk industries such as mining. His approach gained particular attention during the COVID-19 pandemic, as discussed in an episode of LRN's Principled Podcast. Together with Joe Henry, former US Compliance Officer at Braskem, Sullivan shared real-life examples of providing moral leadership in challenging circumstances, showing how values-based decision-making can sustain ethical performance under pressure and strengthen organizational resilience in the face of change. Available at: https://lrn.com/podcast

5.3 Corporate Culture as a Foundation for Compliance Success

A strong corporate culture is widely recognized as a critical factor in ensuring that compliance programs are not just formalities but living systems that guide everyday business behavior. While formal policies and procedures define the rules, it is the organization's shared values, underlying assumptions, and daily practices that ultimately determine whether compliance principles are followed in real situations.

Edgar Schein's model of organizational culture is highly relevant in this context, distinguishing between three levels: artifacts (visible practices such as communication style, office layout, or reporting channels), espoused values (stated principles in mission statements and codes of conduct), and basic underlying assumptions (deeply rooted beliefs and norms that guide decision-making) (Schein, 2010). If there is a gap between what is formally declared and what is informally tolerated, even the most advanced compliance frameworks can be undermined.

Research by Guiso, Sapienza, and Zingales (2015) emphasizes that a culture of corporate trust, where employees believe the organization acts fairly, transparently, and ethically—correlates with higher engagement, reduced misconduct, and better long-term performance. Similarly, Treviño, Weaver, and Brown (2008) highlight that ethical leadership is essential for embedding compliance into organizational culture, as leaders set the tone not only through policies but also through their visible decisions and actions. Kaptein (2015) further argues that effective Chief Ethics and Compliance Officers (CECOs) integrate ethical principles into strategic planning, ensuring that compliance is not treated as a separate control function but as part of the company's strategy.

Practical examples from Europe demonstrate how cultural factors directly shape compliance outcomes. Scandinavian companies such as Nokia (Finland) and Vestas (Denmark) embed transparency into daily operations through open salary structures, public

disclosure of ethical breach reports, and regular staff forums for discussing ethical dilemmas (Transparency International, 2023). These practices normalize open conversations about misconduct and encourage early reporting. In Ukraine, Naftogaz underwent a significant compliance transformation after leadership changes in 2020. The company implemented a third-party-operated whistleblowing hotline, introduced mandatory anti-corruption and conflict-of-interest training, and began publishing annual compliance reports aligned with OECD guidelines (OECD, 2022). Within two years, employee trust surveys and external audits showed measurable improvement, with fewer reported violations and stronger relationships with international partners.

These examples underscore that corporate culture is not a “soft” or secondary factor, it is the foundation on which compliance success is built. Rules and procedures can define what is allowed, but it is culture that determines whether employees feel empowered and motivated to follow them, especially in situations where doing the right thing may not bring immediate commercial benefits. For compliance to thrive, organizations must actively cultivate trust, transparency, and ethical leadership at all levels, making integrity an inseparable part of their business identity.

5.4 Leadership in Compliance: “Tone at the Top” and Leading by Example

Leadership plays a decisive role in shaping how compliance principles are understood, valued, and applied within an organization. The concept of “tone at the top” refers to the ethical climate and behavioral expectations set by senior executives, particularly the CEO and board of directors. If leaders consistently demonstrate integrity, transparency, and fairness, employees are more likely to follow suit; conversely, if leaders are seen tolerating unethical shortcuts, compliance frameworks risk becoming “paper programs” with little practical influence (Kaptein, 2015).

Different leadership styles influence compliance outcomes in distinct ways.

Transformational leaders, who inspire through vision and shared values, often excel at embedding compliance into the corporate culture by making it a central part of the organization’s identity.

Servant leadership, with its focus on listening, empathy, and stewardship, fosters trust and psychological safety, encouraging employees to speak up about misconduct without fear of retaliation (Treviño et al., 2000).

Transactional leaders, while less emotionally driven, can reinforce compliance through clear rules, structured accountability, and consistent enforcement.

Research consistently shows that trust-building is a key factor: when employees believe leadership acts in good faith, they are more willing to align their own behavior with organizational values (Gillespie & Dietz, 2009).

Ethical decision-making at the leadership level requires balancing commercial objectives with regulatory requirements and moral considerations. Leaders are often faced with “gray areas” where the law may be silent, but the ethical implications are significant. The most effective compliance leaders proactively address such dilemmas by

engaging diverse perspectives, consulting with compliance experts, and applying organizational values as decision filters (Brown & Treviño, 2006).

Case in Point: Public Statement Shaping Behavior. *In 2021, the CEO of Siemens AG issued a company-wide video message reaffirming the corporation's zero-tolerance stance on bribery after a global compliance review identified vulnerabilities in certain markets. The CEO's clear, personal commitment combined with follow-up Q&A sessions with employees led to a measurable increase in internal reporting and a 15% rise in employee confidence in compliance processes over the next year (Siemens Sustainability Report, 2022). This illustrates how visible leadership communication can set the tone and reinforce trust across the organization.*

Strong compliance leadership goes beyond formal oversight, it involves consistent role modeling, clear communication, and the courage to make difficult decisions that uphold integrity even in the face of short-term losses. By leading with values and example, executives ensure that compliance is seen not as a constraint but as a source of trust, stability, and sustainable success.

5.5 Practical Tools for Building Ethical Culture

An ethical corporate culture does not emerge spontaneously; it is nurtured through deliberate tools and mechanisms that promote integrity, transparency, and shared responsibility. According to Treviño and Nelson (2021), organizations that successfully integrate ethics into their daily operations rely on a mix of formal structures (e.g., codes, policies) and informal reinforcement (e.g., role modeling, peer influence).

Let's take a closer look at these tools.

Code of Conduct. A well-designed Code of Conduct serves as the primary reference point for employees, outlining expected behaviors, prohibited practices, and the company's commitment to ethical values. It should be accessible, written in clear language, and regularly updated to reflect legal changes and emerging risks. In the EU, codes often include specific clauses on anti-corruption, conflicts of interest, and data protection aligned with GDPR. In Ukraine, the adaptation process frequently involves incorporating requirements from both national legislation and international compliance standards, especially in companies preparing for export or cooperation with EU partners.

Ethics Training – ensures that values are not only stated but understood and applied. Programs may range from onboarding modules to advanced workshops on complex dilemmas. Best practice in European companies includes interactive learning: scenario discussions, role plays, and real-life case analysis. Ukrainian businesses increasingly adapt these methods, integrating local legal contexts and sector-specific risks, such as procurement integrity in public–private projects.

Whistleblowing Channels. Anonymous reporting mechanisms, such as hotlines, secure web portals, or mobile applications, provide employees with safe avenues to report misconduct. The EU Whistleblower Protection Directive (2019/1937) sets minimum standards, including confidentiality and protection against retaliation. In Ukraine,

companies are introducing such channels through specialized providers (e.g., Unified Whistleblower Reporting Portal of Ukraine, Ethicontrol) and ensuring that reports are followed by timely investigation and transparent feedback to the reporter.

Reward Systems for Ethical Behavior. Recognition programs (both financial and symbolic) reinforce the message that ethics and compliance are valued at the highest level. Examples include public acknowledgment during corporate events, certificates for “Ethics Champion of the Month,” or inclusion of compliance metrics in performance evaluations.

Many EU companies operate anonymous hotlines that are monitored by external providers to ensure impartiality. These services are available in multiple languages and supported by training campaigns explaining how to use them effectively. Ukrainian companies, especially in banking, IT outsourcing, and energy, are increasingly adopting this model, adapting it to local labor laws and integrating it with internal compliance functions.

5.6 Measuring and Evaluating Corporate Culture in Compliance

Without systematic assessment, even well-designed policies risk becoming symbolic rather than practical. Effective measurement combines quantitative indicators (such as KPIs and incident reports) with qualitative insights (such as employee perceptions and ethical climate surveys).

Methods and Tools

Employee Surveys – Anonymous questionnaires allow employees to express their perceptions of fairness, leadership integrity, and willingness to report misconduct. Tools like “Ethics Pulse” or culture barometers help track trends over time and reveal emerging risk areas.

Compliance Audits – Regular reviews of processes, training participation rates, and whistleblowing follow-ups ensure that declared policies are embedded into everyday practice.

KPI Tracking – These may include both process metrics (e.g., number of ethics-related trainings delivered, percentage of staff who completed required compliance modules, or time taken to investigate and resolve reported concerns) and outcome metrics (e.g., reduction in repeated violations, improvement in employee perception scores regarding trust and fairness). For example, tracking the volume and type of reported concerns can reveal whether employees feel safe using reporting channels, while monitoring the percentage of business decisions reviewed for compliance risks (such as mergers, procurement deals, or marketing campaigns) can demonstrate the integration of compliance into strategic processes. Over time, consistent KPI monitoring allows organizations to identify patterns, benchmark against industry standards, and adjust programs proactively, ensuring that cultural change is both measurable and sustainable.

Cultural Maturity Models – These are special “development scales” for corporate culture that help companies understand where they currently stand in terms of implement-

ing ethics and compliance. For example, the Ethics Resource Center model describes several stages: from the “initial level” (when ethical rules exist only on paper) to the “mature level” (when ethics and transparency have become a normal part of daily work). Similar tools exist in the EU, such as integrity assessment tools, which allow companies to independently check how well their culture meets current standards and what needs to be improved. It is like a map that shows the path from minimal compliance to full integration of ethics into business.

EU Example

EMD Group, a leading science and technology company headquartered in Germany, conducts regular “High-Impact Culture” Pulse Surveys to assess and improve its corporate culture. These short, targeted questionnaires are distributed to employees across multiple countries several times a year, focusing on topics such as ethical leadership, clarity of compliance policies, and trust in reporting mechanisms. Results are analyzed at both global and regional levels, enabling the company to identify areas for improvement quickly. For instance, when survey data indicated a decline in policy awareness in one European branch, EMD Group implemented focused training sessions and updated communication materials within eight weeks, resulting in a measurable improvement in subsequent survey scores.

Practical Exercises

Exercise 1 – Analyzing the Role of the CECO in Decision-Making

Read the following scenario:

A multinational manufacturing company is considering expanding into a new market. During due diligence, the compliance team identifies those local laws permit certain facilitation payments that are prohibited by the company’s Code of Conduct. The CEO asks the CECO for advice.

> Identify the main compliance risks.

> Propose possible courses of action.

> Justify your recommendation based on corporate values and international compliance standards.

Exercise 2 – Designing a Compliance Awareness Campaign

Work in small groups to create a simple and practical awareness campaign for employees of a mid-sized Ukrainian company that has just introduced a new Code of Conduct. Your task:

> Set clear goals – What should employees know, understand, or do after the campaign?

> Choose at least three communication methods

> Decide how to check the campaign’s effectiveness

Be ready to present your campaign plan to the group and explain why your chosen tools will work.

Exercise 3 – Mapping the culture of compliance Using Edgar Schein's three-level model of organizational culture, analyze the culture of a real organization (indicate the name) that you know.

> Identify visible artifacts

> Determine espoused values

> Infer underlying assumptions and assess whether they support compliance principles.

Draw conclusions about hidden assumptions and assess whether they support the principles of compliance.

Target Questions

1. In what ways can the role of the Chief Ethics and Compliance Officer (CECO) influence strategic decision-making in multinational corporations? Provide examples.
2. How does corporate culture shape employees' willingness to report misconduct, and what mechanisms can strengthen this link?
3. Compare values-based and rules-based approaches to compliance. Which is more effective in high-risk industries and why?
4. How can leadership style at the "top" cascade ethical behavior throughout different levels of an organization?
5. Evaluate the potential conflicts between commercial objectives and compliance requirements. How should leaders balance them without damaging competitiveness?
6. How can compliance organizations measure and improve cultural maturity in a way that supports long-term business sustainability?

List of references for self-study

1. Akinsola, K. (2025). The role of corporate governance in strengthening compliance frameworks. *SSRN.* https://doi.org/10.2139/ssrn.5126938
2. Diligent. (2024). The correlation between corporate governance & compliance. Diligent Blog. https://www.diligent.com/insights/compliance/the-correlation-between-corporate-governance-compliance
3. LRN. (n.d.). How CECOs sustain ethical performance in times of change [Audio podcast episode]. In S. Divers (Host), LRN's Principled Podcast. LRN. https://lrn.com/podcast

4. OECD. (2022). Anti-Corruption Reforms in Ukraine: Pilot 5th Round of Monitoring Under the Istanbul Anti-Corruption Action Plan. OECD Publishing. https://doi.org/10.1787/b1901b8c-en
5. PwC. (2025). Survey results: Out of the back office and into the value chain. Compliance transformation 2025+. Retrieved from https://www.pwc.ch/en/insights/risk/compliance-transformation-2025plus.html
6. Schein, E. H. (2010). Organizational culture and leadership (4th ed.). Jossey-Bass.
7. Siemens AG. (2022). Sustainability report 2022. Retrieved from https://www.siemens.com/sustainability
8. Klevets, O. (2025). Compliance Manager: Who They Are, What They Do, and Why Demand for Their Services Is Growing. *Fin Academy*. Retrieved from https://finacademy.net/ua/materials/article/komplaiens-menedzher [in Ukrainian]

Assignments for Self-study

1. Case Study Analysis: Choose a real-life corporate scandal where compliance failures played a key role (e.g., Volkswagen emissions scandal, Danske Bank money laundering case, UESU financial fraud case, Automagistral-Pivden procurement scandal, Ukrtatnafta/Ukrnafta tax fraud case, Tedis Ukraine monopoly case). Prepare a short paper (2–3 pages) analyzing:
   > What structural or cultural weaknesses led to the failure?
   > How could a stronger CECO function have prevented it?
2. Comparative Research: Compare the compliance culture of a Ukrainian company and an EU-based company in the same sector. Highlight similarities and differences in organizational structures, leadership approaches, and cultural maturity.
3. Interview Assignment: Conduct an interview (in person or online) with a compliance officer, HR manager, or legal advisor. Ask about the challenges of embedding ethics into corporate decision-making. Summarize key insights in a 1-page reflection.
4. Cultural Maturity Assessment: Apply a simplified cultural maturity model to a chosen organization (indicate the name). Assess its stage of ethical culture development and propose three actionable improvements.

Chapter 6: Human Resource Management for Compliance (eg HSEQ)

Learning Outcomes

After studying this chapter, learners will be able to:

- Explain the role of human resource management (HRM) in developing and maintaining an effective compliance culture within an organization.
- Identify how HR policies, recruitment, onboarding, and competence development programs contribute to compliance awareness and ethical behaviour.
- Apply principles of competence management and training, based on ISO 37303:2025, to ensure continuous professional development (CPD) and lifelong learning in compliance.

Key Words: HR policies, competence management, compliance training, capacity building, performance evaluation, recruitment, talent management, HSEQ.

Main Definitions

Human Resource Management (HRM) – a strategic and ethical approach to managing people and organizational culture aimed at aligning workforce policies with compliance, integrity, and performance objectives in accordance with international standards.

Competence Management – a systematic and continuous process of identifying, developing, and evaluating employee knowledge, skills, and behaviours to ensure compliance with legal, ethical, and organizational requirements, supporting continuous professional development (CPD).

HSEQ (Health, Safety, Environment, and Quality) Management – an integrated management system that promotes a safe, ethical, and sustainable workplace by ensuring compliance with health, safety, environmental, and quality standards, and linking them to corporate integrity and social responsibility goals.

Compliance Training and Awareness – structured and interactive educational initiatives designed to build employee understanding of compliance obligations, ethical decision-making, and corporate values, while encouraging proactive risk awareness and integrity in daily work.

Performance Evaluation in Compliance Context – a holistic process for assessing an employee's results, behaviours, and adherence to ethical and compliance standards, integrating Key Performance Indicators (KPIs) that reflect both competence and conduct.

Ethical Leadership – the ability of leaders to influence behaviour and organizational culture by modelling fairness, transparency, and moral courage, ensuring that compliance and digital transformation remain human-centred and sustainable.

Standards, Laws, and Regulations

1. International: ISO 37303:2025 (Compliance management systems — Guidance for competence management); ISO 37301:2021 (Compliance management systems — Requirements with guidance for use); ISO 45001:2018 (Occupational health and safety management systems — Requirements with guidance for use); ISO 14001:2015 (Environmental management systems — Requirements with guidance for use); ISO 9001:2015 (Quality management systems — Requirements).

2. European Union (EU): Directive 2000/78/EC of the Council of 27 November 2000 establishing a general framework for equal treatment in employment and occupation; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation — GDPR); Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (Whistleblowing Directive); Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 on corporate sustainability reporting (Corporate Sustainability Reporting Directive — CSRD).

3. Ukraine: Labour Code of Ukraine; Law of Ukraine "On Occupational Safety"; Law of Ukraine "On Prevention of Corruption; Law of Ukraine "On Ensuring Equal Rights and Opportunities for Women and Men"; Law of Ukraine "On Professional Development of Employees".

List of Subchapters

6.1 The Role of Human Resource Management in Compliance Systems

6.2 Integration of Compliance Principles into HR Policies and Procedures

6.3 Recruitment, Onboarding, and Ethical Induction of Employees

6.4 Competence Management and Continuous Professional Development (CPD)

6.5 Performance Appraisal and Compliance Behaviour Evaluation

6.6 Compliance Training and Awareness Programs

6.7 HSEQ Culture and Employee Engagement in Ethical Practices

6.8 Digital Transformation, Ethical Leadership, and Future Trends in HR Compliance

6.1 The Role of Human Resource Management in Compliance Systems

Human Resource Management (HRM) has evolved from an administrative support function into a strategic pillar of corporate governance and compliance. In today's complex regulatory and ethical environment, people not procedures determine the true level of compliance maturity. As noted by G. Weaver and L. Treviño (2001), the

effectiveness of ethics and compliance programs depends on employees' ethical reasoning, leadership example, and organizational learning.Therefore, HRM is not peripheral to compliance - it is the human engine of integrity, transforming rules into responsible behaviour and culture.

The global shift toward sustainable and ethical business, reinforced by OECD Guidelines for Multinational Enterprises, ISO 37301:2021 and ISO 37303:2025, positions HRM as a strategic partner in risk and ethics management. B. Becker and B. Gerhart (1996), emphasize that HR contributes to long-term compliance resilience by aligning people strategy with corporate governance systems. Within a Compliance Management System (CMS), HRM acts as a connecting link between strategy and behaviour - embedding compliance at every stage of the employee lifecycle. In organizations with mature compliance frameworks, HR managers serve as "compliance custodians":

- participating in the design of Codes of Conduct and ethics policies;
- maintaining competence profiles for compliance-sensitive roles;
- promoting diversity, equality, and inclusion as compliance imperatives;
- coordinating training and communication to build ethical awareness across the workforce.

Ethical compliance begins with hiring decisions. HR ensures fairness, objectivity, and legal conformity following EU Directive 2000/78/EC and Ukrainian equality legislation. In practice, structured interviews, competence-based assessments, and integrity screening ensure candidates' alignment with organizational ethics. Leading companies apply conflict-of-interest and background checks for sensitive roles.

Case in Point: *Ethical Recruitment at Unilever (EU). Unilever integrates compliance criteria into recruitment through digital, bias-free assessments and integrity interviews. Candidates complete ethical values questionnaires ensuring compatibility with the company's Code of Business Principles. This has improved gender balance and reduced grievances related to unfair treatment.*

Onboarding transforms compliance from a rule into a lived value. New employees must understand not only their tasks but also organizational expectations—anti-corruption, data protection (GDPR), safety, and sustainability principles. ISO 37303:2025 identifies competence and awareness as critical components of compliance culture. Progressive HR departments introduce e-learning, ethical handbooks, and case-based workshops.

Case in Point: *Siemens AG (Germany). After its 2006 compliance crisis, Siemens built one of the world's most robust compliance systems, embedding mandatory integrity training into all stages of employee lifecycle. The company's approach—"Only clean business is Siemens business" — has become a model of compliance-driven cultural transformation.*

HR develops competence matrices defining required knowledge, skills, and behaviour for each role. Examples include:

- finance staff – awareness of anti-money laundering (AML) rules;
- procurement – understanding conflict-of-interest prevention;

> managers – ability to identify ethical dilemmas and lead responsibly.

ISO 37303:2025 outlines competence and awareness as pillars of compliance culture. Continuous Professional Development (CPD) ensures regulatory agility, as M. Kaptein (2014) notes, fostering resistance to misconduct.

Performance systems should reward how results are achieved, not only what is achieved. HR integrates compliance indicators into KPIs—such as training participation, tone at the top, and adherence to the Code of Conduct. Example: Microsoft includes ethics and compliance indicators in annual reviews, requiring managers to document evidence of ethical decision-making and reporting transparency.

Trust is the foundation of compliance culture. HR ensures safe reporting channels and non-retaliation in line with the EU Whistleblowing Directive (2019/1937) and Ukrainian anti-corruption laws. HR collaborates with compliance teams on grievance mechanisms, conflict mediation, and consistent disciplinary measures. OECD data and NAVEX benchmarks confirm that organizations with HR engagement in whistleblowing have higher reporting activity and faster resolution rates.

Case in Point: *DTEK (Ukraine). DTEK's HR department co-manages a digital ethics hotline and promotes transparent reporting through external providers. This has improved organizational trust and reduced compliance-related incidents.*

Integrating Health, Safety, Environment, and Quality (HSEQ) principles makes compliance human-centred. Under ISO 45001:2018 and ISO 14001:2015, HR leads initiatives in occupational safety, risk assessment, and mental health. According to the International Labour Organization (ILO, 2024), organizations that foster a strong culture of health, safety, environment, and quality (HSEQ) demonstrate better overall performance, including lower rates of occupational incidents and improved organizational resilience. Human Resources contributes to this by promoting well-being initiatives and integrating sustainability principles into performance evaluation and reward systems.

Digitalization enhances compliance efficiency through HRIS and AI analytics but brings privacy and cybersecurity risks. HR must align systems with GDPR (EU 2016/679) and Ukrainian data protection law.

6.2 Integration of Compliance Principles into HR Policies and Procedures

The integration of compliance principles into Human Resource (HR) policies and procedures is the foundation of ethical and lawful corporate conduct. As G. Weaver and L. Treviño (2001) emphasize, compliance is not achieved solely through control mechanisms but through internalized values embedded in organizational systems. HR policies - covering recruitment, performance, conduct, grievance, and data protection - are the practical instruments through which integrity becomes operational. According to L. Paine (1994), effective compliance programs merge values-based and rules-based approaches - ensuring that ethical behavior is both a moral choice and a formal requirement. The ISO 37303:2025 provides an explicit framework for embedding

compliance principles in all HR processes. It stresses that HR policies should reflect organizational commitment to legality, fairness, and accountability, while ensuring that every employee is aware of compliance responsibilities.

Scholars such as M. Kaptein (2015) note that policy integration is central to shaping ethical behavior because written rules define expectations and boundaries for employees. B. Becker and B. Gerhart (2016) emphasize that HR policies form part of an organization's internal control infrastructure, ensuring that legal and ethical risks are managed systematically. D. Rousseau (1995) highlights that the employment relationship is grounded not only in formal agreements but also in psychological contracts — implicit mutual expectations that underpin trust and commitment. In this context, M. Greenwood (2002) argues that the integration of compliance principles into human resource management establishes an ethical balance between organizational authority and individual rights, turning HR policies into a mechanism for maintaining the social contract within corporate governance.

Key dimensions of compliance integration in HR include:

> policy coherence — alignment of HR rules with legal frameworks and corporate ethics codes;

> procedural fairness — consistency, transparency, and non-discrimination in HR decisions;

> documentation and traceability — evidence of compliance with internal and external regulations;

> feedback and continuous improvement — regular review and adaptation of policies to evolving laws and standards.

Under ISO 37303:2025, organizations must ensure that compliance requirements are systematically translated into HR documentation — including employment contracts, staff manuals, disciplinary codes, and appraisal procedures. In the European Union, HR compliance integration is reinforced by:

> EU Directive 2000/78/EC — equal treatment in employment (EUR-Lex);

> EU Whistleblowing Directive 2019/1937 — internal reporting and anti-retaliation (EUR-Lex);

> General Data Protection Regulation 2016/679 (GDPR) — data processing (GDPR Portal);

> Corporate Sustainability Reporting Directive 2022/2464 (CSRD) — ESG and human rights (EUR-Lex).

These instruments collectively require HR policies that ensure fairness, integrity, and accountability across all levels.

Integration of Compliance in Core HR Procedures:

1. Recruitment and Employment Contracts — anti-discrimination clauses, conflict-of-interest disclosures, ethical hiring.

2. Performance and Conduct Policies — ethical behavior indicators in performance reviews, proportional sanctions.
3. Whistleblowing and Grievance Procedures — secure reporting and protection from retaliation.
4. Data Protection and Record Management — GDPR and national privacy compliance.
5. Health, Safety, and Equality Policies — alignment with ISO 45001:2018, ILO Conventions, and Ukrainian labor laws.

Case in Point: *HR Policy Alignment at Siemens AG (EU). Following major compliance reforms, Siemens revised its global HR policies to align with ISO 37303:2025 and EU directives. Each policy now includes a Compliance and Ethics section defining obligations, reporting procedures, and sanctions (Siemens Integrity and Compliance). Regular audits verify that local HR manuals remain synchronized with global frameworks.*

Ukrainian Legal and Institutional Framework. In Ukraine, compliance integration in HR documentation follows both national laws and EU alignment:

> Labour Code of Ukraine;
> Law “On Prevention of Corruption”;
> Law “On Ensuring Equal Rights and Opportunities for Women and Men”;
> Law “On Personal Data Protection”.

Case in Point: *Ukrenergo (Ukraine). Ukrenergo, the state-owned energy operator, embedded anti-corruption and data-protection clauses into HR policies in 2023 (Ukrenergo Corporate Compliance). Annual audits of compliance documents and training coverage demonstrated a measurable decline in policy violations.*

G. Weaver and L. Treviño (2001) emphasize that ethics and compliance programs cannot operate effectively in isolation from Human Resources, as HR plays a pivotal role in ensuring fairness, transparency, and trust in organizational policies. Their research highlights that collaboration between compliance and HR professionals strengthens employee perception of procedural justice and legitimacy. M. Kaptein (2015) further argues that the effectiveness of ethics and compliance programs depends on their integration into the broader management system, where HR serves as a mechanism for embedding ethical standards into daily practices.

Effective integration between HR and compliance functions involves:

> joint policy drafting — HR ensures clarity and relevance for employees, while compliance guarantees legal and ethical alignment;
> cross-functional committees — HR, Legal, and Compliance officers jointly review policies, assess risks, and manage violations;
> policy training and awareness — HR leads onboarding and refresher programs to build a culture of compliance and integrity;
> monitoring and improvement — regular feedback from audits and employee

surveys informs policy updates and continuous improvement.

Together, these measures create an environment where compliance is not merely a control mechanism but a shared organizational value supported through HR systems and employee engagement.

Case in Point: *HR–Compliance Council at Unilever (EU). Unilever established a joint Ethics & Compliance Council reviewing all HR policies annually (Unilever Business Integrity). The Council includes HR, Legal, and Audit representatives to ensure alignment with global standards. This model has become a benchmark for multinational governance.*

Despite frameworks, integration faces challenges:

- policy fatigue — excessive documentation;
- cultural resistance — compliance perceived as control;
- dynamic regulation — frequent updates;
- balancing confidentiality and transparency. Effective integration requires leadership commitment and communication — policies must be lived, not merely written. This aligns with ISO 37303:2025's values-based compliance philosophy.

6.3 Recruitment, Onboarding, and Ethical Induction of Employees Introduction

Recruitment and onboarding are the first contact points where organisational ethics meet individual values. According to G. Weaver and L. Treviño (2001), the ethical culture of an organisation is strongly influenced by the people hired and the expectations set from day one. Embedding compliance principles in these early stages ensures that every new employee enters the organisation with a clear understanding of legal, ethical and professional obligations.

Standards such as ISO 37303:2025 emphasise that competence-development and awareness must begin prior to employment and continue throughout the employee lifecycle.

M. Kaptein (2015) comprehensive ethics-programs (including codes of conduct, training, monitoring) are associated with lower levels of unethical behaviour. G. Weaver and L. Treviño work (2001) provides a basis for understanding how ethical leadership, culture and socialisation shape employee behaviour.

Together, these scholars argue that HR's early-stage processes (recruitment, onboarding, induction) are decisive for cultivating a workforce committed to lawful, transparent conduct.

Recruitment and induction must comply with national and international laws guaranteeing fairness, non-discrimination and data protection:

European Union:

> Directive 2000/78/EC — equal treatment in employment and occupation.

> General Data Protection Regulation 2016/679 (GDPR) — governs processing of personal data of applicants and employees.

Ukraine:

> Law "On Ensuring Equal Rights and Opportunities for Women and Men" — gender equality.

> Law "On Personal Data Protection" — confidentiality and data processing in HR.

Standards such as ISO 37303:2025 motivate organisations to formalise these compliance elements inside recruitment and induction procedures and to document evidence of ethical orientation and competence verification.

Ethical recruitment integrates compliance from job description to final offer: HR policies must define transparent criteria, objective evaluation methods and anti-bias safeguards. Typical instruments include structured interviews, conflict-of-interest disclosures, integrity screening and GDPR-compliant consent forms. Transparent selection processes increase trust and serve as an informal audit of organisational values.

Onboarding transforms newcomers into responsible insiders. It introduces policies on anti-corruption, data privacy, occupational safety and anti-harassment within the organisation's compliance framework. Effective onboarding includes new-hire sessions on the Code of Conduct and internal control procedures, e-learning modules on GDPR and ethics, signed confirmations of understanding compliance rules and mentor-programmes linking new hires with compliance champions. HR systems document completion rates and assessment results.

Ethical induction extends beyond formal training — it builds a shared sense of purpose and moral accountability. HR must ensure that managers lead by example: explaining why compliance matters, not only what the rules are. Tools may include storytelling of real ethical dilemmas, handbooks linking corporate values to compliance principles, feedback surveys measuring trust and transparency. When newcomers feel psychological safety, they are more likely to speak up — reducing misconduct risk.

Key challenges in ethical recruitment, onboarding and induction include: balancing privacy with background screening; maintaining engagement while ensuring legal conformity; adapting materials for remote/hybrid employees; overcoming cultural scepticism toward compliance training. Organisations must regularly update onboarding content, integrate employee feedback and link lessons from ethics investigations into training updates.

6.4 Competence Management and Continuous Professional Development (CPD)

Competence management and continuous professional development (CPD) represent the core of a sustainable compliance culture. As L. Treviño, G. Weaver, and M. Brown

(2008) emphasize, organizational integrity depends not only on the presence of formal rules but also on the ability of employees to interpret and apply them appropriately. Therefore, the role of Human Resource Management (HRM) in compliance extends far beyond administrative training — it focuses on developing competence frameworks, monitoring ethical performance, and fostering lifelong professional learning.

L. Paine (1994) distinguishes between "rules-based" and "values-based" compliance, arguing that genuine ethical behavior emerges when employees internalize corporate values, not merely obey laws.

M. Kaptein (2015) demonstrates that effective ethics programs combine education, monitoring, and evaluation mechanisms, creating measurable behavioral impact.

R. Boyatzis (2009) defines competence as "an integrated set of knowledge, skills, and attitudes enabling consistent performance across contexts" — a concept directly applicable to compliance-sensitive roles.

As R. Shiri et al. (2023) and A. Friedman (2023) argue, continuing professional development (CPD) transforms compliance from a one-time training event into an ongoing capability-building process, ensuring that employees continually develop the skills, knowledge, and behaviours needed to remain compliant in evolving organisational and regulatory contexts.

Finally, T. Clarke (2022) stresses that competence management supports good governance by aligning employee growth with ethical and legal obligations.

Together, these scholars confirm that competence development is both a compliance requirement and a strategic investment in human capital.

The ISO 37303:2025 establishes a formal link between competence and compliance performance.

It requires organizations to:

- define competence profiles for roles exposed to compliance risks;
- identify knowledge and behavioral requirements (e.g., anti-corruption, data protection, safety awareness);
- evaluate competence through testing, observation, and peer review;
- maintain documented evidence of competence for audit purposes;
- provide continuous training, coaching, and CPD aligned with risk levels.

Competence management ensures that every employee possesses the technical knowledge and ethical awareness necessary to act in conformity with applicable laws and standards.

***Case in Point**: Deloitte operates a Global Compliance Academy, where all professionals complete annual certification in ethics, integrity, and compliance. The program combines ISO-aligned modules, OECD principles, and gamified case simulations that strengthen decision-making under pressure. Learning outcomes are tracked through an integrated Learning Management System (LMS), which links completion data to compliance audit results.*

In the European Union, competence management aligns with several strategic frameworks:

- EU Skills Agenda (2020) — supports lifelong learning and ethical employability;
- European Qualification Framework (EQF) — links competence levels with professional standards;
- ISO 45001:2018 — requires demonstrated competence in occupational health and safety management;
- EU Whistleblowing Directive (2019/1937) — mandates awareness and training on reporting procedures and protection rights.

In Ukraine, competence development and CPD are governed by:

- Labour Code of Ukraine — requires ongoing qualification improvement;
- Law “On Professional Development of Employees” — defines formal and informal CPD formats;
- Law “On Prevention of Corruption” — establishes training duties for anti-corruption officers;
- Human Development Strategy — emphasizes competence-based education and professional ethics.

Ukrainian universities and enterprises increasingly integrate compliance, safety, and ethical modules into HR development systems, reflecting EU alignment.

CPD transforms compliance into a dynamic learning ecosystem. CPD enhances ethical reflexivity — the ability to adjust behavior to evolving laws, technologies, and social expectations.

ISO 37303:2025 recommends documenting all CPD activities (training, mentoring, e-learning, external certification) and linking them to compliance key performance indicators (KPIs).

An effective CPD framework includes:

- annual training plans based on risk assessment;
- specialized courses for high-risk departments (finance, procurement, data protection);
- leadership programs promoting ethical decision-making;
- cooperation with universities and certification bodies;
- evaluation of CPD impact through audits, surveys, and HR analytics.

Digital transformation further strengthens CPD through AI-driven personalization and automated tracking of competence gaps.

The main challenges for integrating competence management and CPD include:

- lack of certified trainers and accredited programs;

- balancing regulatory obligations with learning flexibility;
- measuring qualitative impact on ethical culture;
- preventing “compliance fatigue” caused by over-formalization.

6.5 Performance Appraisal and Compliance Behaviour Evaluation Introduction

Performance appraisal is one of the key instruments through which organizations align ethical values with employee behaviour.

Traditional evaluation systems focus on what employees achieve — productivity, sales, efficiency. In compliance-oriented management, equal importance is given to how these results are achieved.

Therefore, assessing compliance behaviour transforms performance management from a transactional tool into a mechanism of ethical governance.

L. Paine (1994) distinguishes between compliance-based systems that rely on sanctions and integrity-based systems that encourage responsible behaviour through shared values.

M. Kaptein (2015) analyzes the impact of the scope, composition, and sequence of ethics program components on the frequency of unethical behavior, thereby proposing an operationalization of ethical performance through measurable components that can serve as proxy indicators of fairness, transparency, and integrity.

M. Armstrong & S. Taylor (2021) emphasise that modern performance management must be continuous, evidence-based, and developmental.

T. Clarke (2021) argues that corporate-governance frameworks increasingly embed value-driven mechanisms, thereby rendering values into observable action and enhancing organisational integrity.

Together these perspectives confirm that HR appraisal systems must measure both competence and conduct to sustain ethical performance.

The ISO 37303:2025 requires that compliance objectives be reflected in HR performance frameworks by:

- linking appraisal metrics to ethical conduct;
- recording compliance evidence in performance documentation;
- incorporating compliance goals into management reviews;
- ensuring privacy protection in evaluation (GDPR 2016/679).

Additional relevant frameworks:

- ISO 45001:2018 — integration of health-and-safety performance indicators;
- EU Corporate Sustainability Reporting Directive (CSRD 2022/2464) — mandates ESG-related metrics, including governance and ethics;

- Law of Ukraine “On Prevention of Corruption” — requires ethical criteria in public-sector evaluations;
- Law of Ukraine “On Public Service” — introduces integrity as an appraisal dimension.

HR departments bridge compliance principles and measurable performance by:

- designing appraisal frameworks that include ethical indicators;
- training managers to evaluate behaviour objectively;
- ensuring uniform application across units;
- maintaining documentation for internal and external audits.

Common compliance-linked indicators include:

- adherence to internal controls and reporting obligations;
- participation in ethics and compliance training;
- demonstration of ethical leadership (“tone at the top”);
- contribution to diversity, inclusion, and psychological safety;
- absence of disciplinary sanctions or conflict-of-interest breaches.

Case in Point: *Siemens AG (Germany). Following comprehensive compliance reforms initiated after 2006, Siemens AG integrated integrity and risk-management principles into its corporate governance and human resource practices. Managers are assessed not only for business results but also for their commitment to compliance training, ethical leadership, and transparent reporting. Compliance and ESG criteria have been incorporated into the company’s executive remuneration system, linking integrity and responsible conduct to long-term performance outcomes.*

Effective compliance appraisal requires balanced KPIs combining quantitative and qualitative elements:

- completion rates of compliance or HSEQ training;
- number and timely resolution of ethical issues;
- employee-survey results on trust and ethical climate;
- documentation of compliance discussions in team reviews.

M. Kaptein (2015) cautions that indicators must promote ethical reflection, not checkbox conformity.

Modern approaches to performance and compliance management emphasise behavioural criteria — including consistency, transparency, and mutual trust — as stronger predictors of an ethical and responsible organisational culture.

Case in Point: Microsoft (Global). Microsoft’s Performance and Development Approach (PDA) focuses on how employees achieve results through the principles of “Model, Coach, Care.” The approach encourages managers and employees to demonstrate

accountability, respect, and integrity in daily decisions and interactions. Ethical and inclusive behaviour is an explicit expectation for all roles, and performance reviews incorporate discussion of how these values are applied in practice. This behavioural assessment influences employees' development plans, promotions, and rewards.

Modern HR systems employ mixed methods to evaluate compliance behaviour:

- 360° Feedback from peers and subordinates on ethical conduct;
- behavioural Observation Scales (BOS) for visible compliance actions;
- ethical Self-Assessment surveys encouraging moral reflection;
- audit Integration linking appraisal data to internal control findings;
- digital Analytics ensuring GDPR-compliant monitoring of training and alerts.

In Ukrainian organizations within the energy, banking, and telecommunications sectors, there is a growing trend toward integrating compliance elements into performance management systems.

In practice, this is reflected in the following areas:

- embedding ethical standards and principles of integrity in job descriptions, corporate codes of conduct, and evaluation forms;
- conducting regular training sessions and self-assessments of awareness in compliance, anti-corruption policy, and data protection;
- considering HSEQ indicators (health, safety, environmental responsibility, and quality) and adherence to anti-corruption norms in strategic planning and KPI management processes;
- implementing material and non-material reward systems that take into account discipline in observing ethical and legal requirements.

However, the process of embedding compliance principles into performance management frameworks is not without challenges. The following issues illustrate the key areas where further improvement and adaptation are needed.

Current challenges include:

- cultural resistance where staff perceive monitoring as control;
- difficulty quantifying ethical behaviour;
- managerial bias in subjective ratings;
- over-formalisation reducing open dialogue.

M. Armstrong and S. Taylor (2021) highlight that modern performance management should be a continuous and developmental process supported by regular coaching and constructive feedback rather than traditional annual reviews.

In turn, T. Clarke (2021) emphasises that corporate governance and compliance systems are most effective when they embed ethical dialogue, transparency, and accountability into everyday management practices.

Together, these approaches transform compliance from a control mechanism into a

process of learning and professional growth.

When properly integrated, compliance-based appraisal yields measurable outcomes:

> stronger ethical culture and psychological safety;

> increased stakeholder trust and transparency;

> higher engagement and retention;

> lower reputational and legal risk;

> alignment of HR systems with ESG and sustainability goals.

Empirical experience and organizational practice demonstrate that companies integrating integrity and ethical behaviour into performance evaluation frameworks tend to achieve higher levels of trust, adaptability, and long-term resilience.

6.6 Compliance Training and Awareness Programs Introduction

Compliance training and awareness initiatives form the educational foundation of every Compliance Management System (CMS). While Codes of Conduct establish ethical and legal standards, structured training ensures that employees understand, internalize, and apply these standards in daily practice. Awareness programs, in turn, complement formal learning by embedding integrity into everyday communication and reinforcing a culture of ethical vigilance across all levels of the organisation.

ISO 37303:2025 recognises competence and awareness as fundamental CMS requirements, emphasizing that compliance capability must be maintained through continuous learning rather than one-off instruction. Effective programs adapt to evolving risks, roles, and regulatory expectations, ensuring that every employee remains aware of their compliance responsibilities.

L. Paine (1994) distinguishes between compliance-based (rules-oriented) and integrity-based (values-oriented) ethics strategies, suggesting that sustainable compliance arises when legal obligations are reinforced by moral reasoning and ethical reflection.

Similarly, M. Kaptein (2015) finds that the effectiveness of ethics programs depends on their comprehensiveness: initiatives that combine training, communication, and accountability mechanisms are more successful in reducing unethical behaviour and enhancing employees' ethical awareness.

WT Jr. Branch and M. George (2017) demonstrate that reflection-based learning supports professional ethical formation by encouraging behavioural transformation through self-examination and feedback — principles equally applicable to compliance education, where learning aims to shape ethical judgement and responsible conduct.

Reinforcing this, R. Sims (2002) identifies experiential pedagogy — such as simulations, role-playing, and case-based exercises — as a cornerstone of effective ethics education, enabling learners to translate knowledge into consistent ethical behaviour.

Hence, compliance education serves both knowledge transfer and cultural formation.

According to ISO 37303:2025 organisations should:

> deliver training proportionate to compliance risks and roles;

> ensure all personnel understand their compliance duties and decision-making responsibilities;

> maintain verifiable records as audit evidence;

> evaluate effectiveness through assessments, surveys, and analysis of incident trends.

Through the integration of structured training and continuous awareness initiatives, organisations embed compliance values into everyday communication and cultivate a sustainable culture of integrity. Taken together, these frameworks and scholarly perspectives outline the conceptual foundation of compliance education, highlighting its dual role as both a preventive and developmental function within organisations.

However, to ensure that compliance training delivers measurable results, it must be guided by clearly defined objectives that connect learning outcomes with ethical performance and risk management.

The main objectives of compliance training include:

1. Knowledge development - understanding laws, regulations, and policies;
2. Behavioural change - promoting ethical conduct;
3. Risk mitigation - reducing corruption or data-breach incidents;
4. Cultural reinforcement - embedding integrity into identity;
5. Audit readiness - maintaining competence evidence.

Empirical research confirms that well-structured HRM programs enhance employee engagement and support a culture of responsibility.

Case in Point: *Deloitte Ethics & Compliance Learning Journey. Deloitte implements a global ethics-training framework that combines foundational modules and role-specific curricula. According to Deloitte's public disclosures, ethics training is required for all new hires upon joining, upon promotion to certain levels, and for all Deloitte people every two years. The programme includes a mix of online courses, virtual and classroom sessions, and interactive case discussions. In addition, Deloitte promotes broader topics such as data privacy and information security through its privacy awareness campaigns and training. Training effectiveness is supported by annual ethics surveys, internal reviews, and confirmation of compliance with the Global Code of Conduct.*

This integrated approach reflects how leading organisations align diverse learning methods with compliance objectives. To achieve similar effectiveness, compliance education should employ a variety of delivery formats (Table 6.1) - each reinforcing ethical understanding through different forms of engagement and feedback.

Table 6.1 Methods and Formats of Training

Method	Example
E-learning	Scalable GDPR or anti-bribery modules
Workshops	Interactive case discussions
Microlearning	Short, targeted digital lessons
Simulations / Gamification	Ethical-pressure role play
Mentoring	Ethical coaching by senior leaders
Campaigns	Visual or video-based awareness
Surveys	Measure knowledge and perception

L. Paine (1994) and R. Sims (2002) show that interactive, context-specific learning produces stronger retention. Hybrid delivery (digital + in-person) ensures inclusivity for remote teams.

By combining these methods, organisations create a continuous learning ecosystem that not only transfers knowledge but also reinforces ethical behaviour.

However, to ensure that such programs deliver tangible results, their impact must be systematically measured and analysed.

According to M. Armstrong and S. Taylor (2021), training should be evidence-based and aimed at achieving measurable outcomes.

Evaluation metrics include:

- knowledge-test and certification results;
- decrease in misconduct or repeat violations;
- employee-survey results on ethical confidence;
- manager feedback on behavioural improvement;
- linkage between training participation and audit outcomes.

M. Kaptein (2015) emphasizes that the impact of ethics programs should be evaluated over time, as cultural and behavioural change requires longitudinal observation rather than short-term knowledge measurement.

Case in Point: *Unilever Business Integrity Programme. Unilever operates a global Business Integrity Programme designed to embed ethical values and responsible conduct into employees' everyday work. The programme includes mandatory training modules for all employees, supported by regional and role-specific materials. In 2023, Unilever launched a new multilingual version of its integrity training that applies a storytelling-based approach to engage learners through realistic scenarios. Completion and compliance rates are monitored through an online learning platform, and continuous communication on ethical conduct is reinforced through the company's global Speak Up channels and internal campaigns. A comprehensive integrity programme such as*

Unilever's demonstrates that compliance education does not end with formal training modules.

To truly embed ethical values in everyday behaviour, organisations must go beyond structured learning.

Awareness requires continuous communication and visible leadership, as T. Clarke (2021) emphasizes that transparent communication, values-based leadership, and a strong ethical culture help sustain long-term organizational commitment.

Typical tools: newsletters, "Integrity Days," short videos, ethics ambassadors, and intranet campaigns. Such initiatives humanise compliance and keep ethics emotionally relevant.

Ukrainian corporations and public institutions are gradually developing structured approaches to compliance and integrity education.

Examples include:

- corporate ethics and compliance programs within Naftogaz Group, supported by its Code of Ethics and internal Compliance Office;
- integrity and transparency initiatives introduced by Ukrenergo, PrivatBank, and the National Bank of Ukraine, aiming to strengthen ethical culture in management and decision-making;
- national anti-corruption and integrity e-learning platforms launched by the National Agency on Corruption Prevention (NACP), such as the Study.NAZK platform;
- awareness-raising efforts and national legislation promoting gender equality and the prevention of workplace harassment, supported by cooperation between government bodies and international partners.

These initiatives demonstrate a gradual shift from a formal, rule-based approach to compliance toward proactive ethical education and integrity culture-building across both corporate and public sectors in Ukraine.

The growing number of compliance and integrity initiatives demonstrates meaningful progress in shaping ethical awareness across Ukraine's corporate and public sectors. However, alongside these achievements, several systemic and practical challenges remain that require further attention to ensure the long-term effectiveness and sustainability of compliance education.

Persistent challenges include:

- limited localisation of global training materials;
- training overload leading to "compliance fatigue";
- insufficient measurement of long-term learning impact;
- shortage of certified compliance trainers.

Emerging trends include:

- AI-driven adaptive learning platforms;
- integration of training analytics into performance management systems;

- > expansion of experiential and simulation-based ethics training supported by digital technologies;
- > growing professionalisation and certification of compliance educators and trainers.

6.7 HSEQ Culture and Employee Engagement in Ethical Practices Introduction

The concept of HSEQ — Health, Safety, Environment, and Quality — extends beyond technical compliance and procedural control, encompassing the broader domain of organizational ethics. A mature HSEQ culture ensures that business operations safeguard human life, protect the environment, and promote transparency and accountability in quality management processes.

As L. Treviño and K. Nelson (2021) emphasize, ethical organizations perceive HSEQ not as a regulatory checklist but as a moral contract with employees and society, reflecting shared values of care, respect, and responsibility. Accordingly, compliance and HSEQ culture are inseparable dimensions of integrity management — both rely on continuous awareness, ethical leadership, and active employee engagement.

According to E. Schein (2010), organizational culture represents “a pattern of shared basic assumptions learned by a group as it solves problems of external adaptation and internal integration.” Applied to HSEQ, culture becomes the invisible framework guiding safe, responsible, and ethical behavior throughout the organization. It determines how individuals interpret risk, respond to hazards, and prioritize human and environmental well-being in daily decisions.

J. Reason (1997), in his renowned Swiss Cheese Model, demonstrated that most accidents arise not from individual negligence but from systemic weaknesses — including fear, underreporting, or the normalization of deviance. In this view, the absence of an open and ethical safety culture creates preconditions for failure, while a transparent environment that encourages speaking up significantly reduces the likelihood of incidents.

L. Paine (1994) and M. Kaptein (2015) further argue that both ethical lapses and safety failures originate in a tolerance for minor deviations from established standards. When small breaches are overlooked, they gradually erode ethical norms and operational discipline, leading to serious organizational consequences.

R. Knode (2020) reinforces this perspective by showing that employee engagement is a critical determinant of safety culture maturity. Higher levels of participation in safety-culture models indicate that organizations perceive HSEQ not merely as procedural compliance but as a shared ethical commitment between management and employees. This engagement strengthens trust, accountability, and collective responsibility for outcomes.

Similarly S. Clarke (2006) and M. Christian et al. (2009) demonstrate that stronger employee participation and compliance within a positive safety (HSEQ) climate are associated with improved safety performance and fewer incidents. Such findings

confirm that engagement functions as a behavioral and moral mechanism linking individual actions with organizational integrity and long-term sustainability.

Taken together, these perspectives depict HSEQ culture as an ethical ecosystem — one sustained through ethical leadership, reflective learning, and shared responsibility. Organizations that cultivate such a culture move beyond mere legal conformity toward proactive stewardship of people, society, and the environment, embedding ethics into every aspect of operational practice.

The ethical foundations of HSEQ culture provide the conceptual basis for how organizations perceive and implement safety, environmental, and quality responsibilities. However, translating these values into consistent practice requires formal structures and clearly defined standards. Therefore, international, regional, and national regulatory frameworks play a decisive role in institutionalizing HSEQ ethics — establishing mandatory requirements that transform ethical principles into verifiable compliance obligations.

Global and national frameworks ensure that ethical aspirations for HSEQ are supported by enforceable legal and procedural instruments. These standards not only regulate operational processes but also reinforce the moral dimension of safety, environmental stewardship, and quality management.

International standards:

- ISO 45001:2018 – Occupational Health and Safety Management Systems;
- ISO 14001:2015 – Environmental Management Systems;
- ISO 9001:2015 – Quality Management Systems;
- ISO 37303:2025 – Compliance management systems;
- ILO Conventions 155 and 187 – Occupational Safety and Health Promotion.

European Union:

- EU OSH Framework Directive 89/391/EEC – mandates worker safety, consultation, and participation;
- European Green Deal (2019) and Corporate Sustainability Reporting Directive (CSRD 2022/2464) – require transparency in environmental and social performance, linking sustainability and accountability to corporate governance.

Ukraine:

- Law “On Labour Protection”;
- Law “On Environmental Protection”;
- Law “On Technical Regulations and Conformity Assessment”.

Collectively, these frameworks transform HSEQ from a voluntary initiative into a comprehensive system of legal and ethical governance. They ensure that organizational performance, risk management, and sustainability commitments align with the fundamental responsibility to protect people, society, and the environment.

An ethical HSEQ culture integrates moral values - responsibility, transparency, and care - into every business process.

As L. Paine (1994) explains, an integrity-based approach encourages individuals and organizations to act in accordance with shared ethical values out of internal conviction rather than external control. This perspective highlights that compliance excellence depends not only on adherence to standards, but also on the moral will to “do what is right” as a matter of principle and conscience.

Translating ethical intent into consistent behavior requires coordinated institutional mechanisms.

Accordingly, HR and compliance departments jointly foster such culture by:

- embedding HSEQ values in policies and training;
- promoting a “zero-harm” philosophy and psychological safety;
- ensuring non-retaliation for incident reporting;
- rewarding proactive safety and sustainability initiatives;
- linking HSEQ behaviour to performance appraisals.

Ethical leadership plays a decisive role: M. Kaptein (2015) demonstrates that integrity-based leadership reduces violations and enhances trust in reporting systems.

Case in Point: *S*hell Europe (Netherlands). Shell’s long-term Goal Zero program integrates ethics and safety into everyday operational decision-making, aiming for zero harm to people and the environment. All employees and contractors are required to complete Life-Saving Rules training, which defines critical safety behaviours and personal accountability. The company systematically promotes learning through “Safety Moments” - short discussions at the start of meetings where employees reflect on real-life incidents, preventive actions, or near-misses. This practice fosters shared responsibility and continuous ethical awareness of risk.

According to the Shell Sustainability Report 2023, the company has maintained one of the lowest rates of work-related injuries in its industry, reporting a continued downward trend in Lost Time Injury Frequency (LTIF) over the past decade and recording zero fatal incidents under Shell’s operational control in 2020. The program demonstrates how safety culture and ethical leadership can be jointly embedded into HSEQ performance systems.

The experience of companies such as Shell demonstrates that a strong HSEQ culture cannot be sustained solely through policies or leadership — it requires continuous participation and commitment at every organizational level. Employees play an active role in translating ethical and safety principles into daily behaviour, making engagement a cornerstone of effective compliance and risk management.

Employee engagement transforms compliance from an external control mechanism into a system of shared accountability.

J. Reason (1997) noted that reliable risk management depends on an organization’s ability to anticipate and identify latent system weaknesses before they lead to incidents.

Such a proactive approach to risk is built on shared attentiveness, mutual support, and open communication within teams. When employees are actively engaged in safety management, they do not merely comply with procedures but take conscious responsibility for preventing errors and reducing risks. Therefore, employee engagement becomes a critical factor in shaping HSEQ culture and compliance systems grounded in trust, accountability, and shared values.

Practical strategies for engagement include:

- employee-led safety committees and risk assessments;
- "Stop Work Authority," enabling employees to suspend unsafe tasks;
- internal suggestion systems for safety and ethics improvements;
- recognition programs rewarding ethical leadership and safe conduct.

As S. Clarke (2006) demonstrates, a positive safety climate — supported by employee involvement and shared responsibility — significantly enhances safety performance. Engaged employees act as social influencers who reinforce safe and ethical behaviour among their peers.

Case in Point: Siemens Energy (Germany). Siemens Energy has implemented a 24/7 "Speak Up" reporting channel - available to both employees and external parties - allowing anonymous submissions of suspected compliance or safety violations. This approach illustrates how modern HSEQ/compliance systems can be integrated into corporate culture through employee participation, open communication, and building trust. The experience of Siemens Energy demonstrates that ethical and safety integrity cannot be achieved through isolated initiatives alone. Sustaining a mature HSEQ culture requires systemic alignment — where compliance, occupational safety, and environmental management operate as interconnected elements of a unified framework.

To support this integration, international standards such as ISO 37303:2025, ISO 45001:2018, and ISO 14001:2015 establish a shared foundation built on competence, leadership, and continual improvement.

ISO standards underline the interdependence of compliance, health, safety, and environmental management. When implemented together, these frameworks evolve into Integrated Management Systems (IMS) that strengthen organizational coherence and ethical accountability.

Integrated systems typically:

- unify risk registers across HSEQ and compliance;
- standardize audit and reporting procedures;
- employ digital dashboards for joint performance monitoring;
- cross-train staff in ethical and technical domains to reinforce a shared responsibility culture.

As B. Becker and B. Gerhart (2016) emphasize, the integration of organizational systems and HR practices strengthens internal communication, minimizes functional duplication, and enhances organizational adaptability and resilience.

Ukrainian enterprises are aligning HSEQ culture with EU sustainability and compliance standards.

This process is reflected in the initiatives of leading Ukrainian companies and institutions that integrate ethical, environmental, and safety standards into their operational practices.

Examples include:

- Ukrenergo – implementing a formal Compliance Program and Code of Ethics that define integrity and accountability policies. The company also operates an Integrated Management System (IMS) certified to ISO 9001, ISO 14001, and ISO 45001 standards, covering environmental management, occupational health and safety, and ethical governance practices;
- ArcelorMittal Kryvyi Rih – maintaining an ISO 14001:2015-certified environmental management system and publicly disclosing information on ecological performance through its Ecology platform, illustrating the company's commitment to transparency and environmental responsibility;
- Naftogaz Group – embedding corporate ethics and compliance standards through its Ethics and Compliance Policy and public governance framework, demonstrating how compliance principles are integrated into the company's operational and decision-making structures.

Together, these initiatives illustrate Ukraine's gradual alignment with European standards of responsible business conduct, transparency, and ethical governance within the corporate sector. They show how Ukrainian enterprises are not only adopting technical HSEQ and compliance frameworks but also institutionalizing ethical leadership and integrity across their management systems.

However, achieving a mature HSEQ culture requires not only formal adoption of standards but also systematic evaluation and continuous improvement.

Assessing HSEQ culture involves both quantitative and qualitative metrics:

- safety and environmental performance indicators (accident, emissions, waste data);
- employee surveys on ethical climate and trust;
- audit results of training and reporting participation;
- qualitative feedback analysis.

T. Garavan (2019) recommends continuous assessment combining "hard" KPIs with "soft" indicators of ethical maturity.

Advanced organizations employ Culture Maturity Models, evolving from compliance-based to value-based safety cultures.

The continuous assessment of HSEQ culture not only helps identify areas of improvement but also provides valuable insights into how organizations evolve from compliance-driven structures to value-driven ethical ecosystems.

However, maintaining such progress requires overcoming several systemic and

behavioural challenges that continue to limit the maturity of HSEQ and compliance integration.

Despite progress, challenges persist:

- insufficient coordination between compliance and HSEQ teams;
- focus on documentation rather than behaviour;
- limited empowerment in reporting;
- resistance to cultural transformation.

Emerging trends include:

- AI-driven predictive safety analytics;
- integrated ESG–HSEQ dashboards;
- gamified learning for ethical awareness;
- alignment of HSEQ ethics with the UN Sustainable Development Goals (SDGs).

The further development of HSEQ and compliance systems requires not only the technical improvement of management mechanisms but also the cultivation of a mature organizational culture in which ethical responsibility, transparency, and safety serve as strategic determinants of sustainable development and stakeholder trust.

6.8 Digital Transformation, Ethical Leadership, and Future Trends in HR Compliance

Digital transformation and ethical leadership have become key drivers of HR compliance development.

Automation, analytics, and artificial intelligence (AI) are increasingly influencing recruitment, learning, and performance management — creating new opportunities for efficiency while simultaneously generating complex challenges for ethical governance.

Global trends such as the integration of ESG principles, the expansion of remote work, and growing demands for data transparency are reshaping the paradigm of corporate responsibility.

In contemporary management, ethics is increasingly viewed not as a system of control but as a strategic resource of trust, reputation, and sustainable growth.

Therefore, future-oriented HR compliance must combine technological progress with a human-centered approach to leadership, ensuring that data-driven systems strengthen integrity rather than control.

Digital compliance in the field of human resource management is increasingly viewed as a synthesis of technological innovation and ethical principles of corporate governance.

It represents a shift from a reactive to a proactive approach to compliance, where digital tools - such as people analytics, artificial intelligence, and learning management

systems - are applied not merely for control but for risk prediction and the development of a culture of trust.

As emphasized by M. Brown, L. Treviño, and D. Harrison (2005), ethical leadership involves the demonstration of normatively appropriate conduct through personal actions and interpersonal relationships, setting the moral tone for the entire organization.

M. Kaptein (2008) defines ethical culture as a system of virtues that supports conscious decision-making and promotes responsible behavior even in complex technological environments.

L. Paine (1994) stresses that effective compliance should be based not on coercion but on an internal motivation for integrity — a principle that ensures the resilience of ethical decision-making in the digital era.

Responsibly implemented HR analytics can serve as an effective mechanism for the early detection of ethical and regulatory risks, provided that technological solutions are combined with the principles of transparency, fairness, and respect for human dignity.

These conceptual foundations of ethical and digital compliance are reinforced by a system of international and national frameworks that formalize integrity, transparency, and accountability in corporate governance.

The following international and national frameworks provide the regulatory foundation for digital HR compliance.

International and EU Frameworks:

- ISO 37303:2025 – Compliance management systems — Guidance for competence management: integrates competence, ethics, and leadership as foundations of responsible governance;
- ISO 37000:2021 – Governance of organizations — Guidance: promotes ethical purpose, integrity culture, and stakeholder trust;
- GDPR (EU Regulation 2016/679) — regulates lawful processing of personal and biometric data;
- EU Artificial Intelligence Act (2024) — establishes transparency, fairness, and human-oversight standards for AI use in HR and compliance;
- OECD Guidelines for Multinational Enterprises (2023 update) — promote responsible business conduct, whistleblower protection, and due diligence.

Ukraine:

- Law “On Personal Data Protection” — harmonized with GDPR;
- Law “On Electronic Identification and Electronic Trust Services” — governs digital identity and signatures;
- Human Development Strategy — emphasizes competence-based and ethical leadership;

> Strategy for the Digital Development of Innovation Activity of Ukraine — aligns Ukraine's governance with EU standards for data ethics and transparency.

Building on these regulatory and ethical frameworks, organizations are increasingly implementing digital tools that translate compliance principles into daily HR practices.

These technologies operationalize the requirements of ISO, GDPR, and national legislation, enabling transparency, accountability, and data-driven monitoring of ethical behaviour.

The most widely used instruments in digital HR compliance include the following systems and platforms (Table 6.2).

Table 6.2 Digital Tools and Technologies for HR Compliance

Digital Tool / System	Compliance Function
Learning Management Systems (LMS)	Track participation in compliance and ethics training.
HR Analytics Platforms (SAP SuccessFactors, Workday)	Monitor adherence to policies, diversity metrics, and turnover risks.
Automated Whistleblowing Portals	Enable anonymous, GDPR-compliant reporting.
AI-based Recruitment Engines	Detect bias and conflicts of interest during hiring.
Digital Document Management Systems (DMS)	Maintain secure audit trails and version control.
Predictive Analytics Dashboards	Identify early-warning signals of compliance breaches.

In summary, the implementation of digital tools in HR compliance enhances the accuracy, transparency, and accountability of processes, provided that ethical principles of technology use are respected and appropriate oversight mechanisms are in place.

Case in Point: *Deloitte and Predictive Compliance Analytics. Deloitte applies compliance analytics within its HR and risk-management systems to identify behavioral and operational anomalies while ensuring data privacy through minimization protocols. According to the company's publicly available ethics and integrity materials, the use of predictive dashboards has enhanced transparency and responsiveness in compliance oversight. While digital compliance tools strengthen control and transparency, their effectiveness ultimately depends on the ethical judgment of those who design, implement, and oversee them.*

Technology alone cannot guarantee integrity - it requires leaders who understand the moral implications of automation and ensure that innovation serves human values

rather than replacing them. This brings the discussion to the next essential dimension of digital transformation - ethical leadership in the digital compliance era.

Ethical leadership bridges the gap between automation and accountability.

In practice, ethical leaders:

> promote openness and learning from mistakes;

> model responsible data use and transparency;

> empower employees to question unethical automation;

> integrate ethics into innovation and digitalization;

> communicate purpose and meaning, not merely policy.

As M. Brown, L. Treviño, and D. Harrison (2005) note, ethical leaders define organizational ethics through what they reward, tolerate, and exemplify — translating integrity into everyday managerial practice. Their actions and decisions set the moral tone of the organization, signaling which behaviors are valued and which are unacceptable. Therefore, HR-compliance leadership must foster dialogue, empathy, and shared responsibility to sustain an ethical culture.

Therefore, HR-compliance leadership must foster dialogue, empathy, and shared responsibility to sustain ethical culture.

Case in Point: *SAP (Germany). SAP's "Responsible AI" framework aligns its HR-analytics and recruitment AI-tools with data-privacy, transparency and fairness principles. The company states that before deploying AI-based recruiting and people-analytics solutions it implements governance and oversight mechanisms (for example an internal AI ethics committee). On the careers site SAP emphasises the ethical usage of AI in recruiting, including commitment to transparency, data-privacy and alignment with HR compliance practices.*

The compliance landscape is evolving rapidly under digital, social, and sustainability influences.

Key global trends include:

> aI-driven compliance monitoring — predictive models detecting misconduct before it occurs;

> integration with ESG governance — linking compliance indicators to environmental and social metrics;

> algorithmic transparency — mandatory audits of AI-based HR decisions;

> human-centered leadership — empathy, inclusion, and psychological safety as compliance competencies;

> hybrid-work compliance — policies for digital conduct, cybersecurity, and cross-border employment;

> ethical sustainability reporting — ESG dashboards tracking integrity and stakeholder trust.

In the coming years, compliance will gradually evolve into a measurable system of ethical performance that integrates legal, social, and managerial dimensions of responsibility.

Ukraine is gradually developing its digital compliance and ethics infrastructure, aligning national initiatives with European standards of transparency, accountability, and data protection.

A notable example is the Naftogaz Group, which has implemented SAP S/4HANA and SAP Business Planning and Consolidation solutions to improve data management, transparency, and reporting integrity. These technologies support corporate governance reforms and strengthen internal control and compliance processes.

At the state level, the Ministry of Digital Transformation of Ukraine promotes ethical and transparent digital governance. In 2024, it released the White Paper on Artificial Intelligence Regulation in Ukraine, outlining the national framework for ethical AI, data protection, and accountability in public administration. This document reflects Ukraine's commitment to European principles of responsible digital transformation and human-centered AI development.

Together, these initiatives demonstrate Ukraine's progress toward European-aligned digital compliance, emphasizing integrity, technological transparency, and respect for human rights in both corporate and public sectors.

However, this progress coexists with persistent challenges — including the need for ethical oversight of AI and analytics, the elimination of data-protection infrastructure gaps, and the strengthening of competence development in compliance leadership. Addressing these challenges requires a systemic approach to leadership learning and capacity building.

According to ISO 37303:2025, organizations must ensure continuous competence development in ethics, governance, and compliance. Key learning domains include ethical reasoning and decision-making, data ethics and digital literacy, stakeholder communication, resilience and psychological safety, as well as systems thinking and ESG integration.

Leadership learning, therefore, should be designed as an ecosystem that integrates formal education, mentoring or coaching, and structured reflective practice. Yet even in organizations that develop such ecosystems, ethical principles often remain difficult to translate into consistent behaviour.

Common difficulties include balancing automation efficiency with ethical oversight, preventing leadership fatigue during crises, ensuring cross-cultural consistency of ethical standards, and bridging the gap between regulation and values-based practice.

The future of HR compliance will thus depend on adaptive, human-centred leaders who perceive integrity not as an administrative obligation but as a continuous learning journey. Ethical capacity-building will remain as essential as technological innovation, shaping organizations where compliance sustains trust — not control.

Practical Exercises

Exercise 1 – Identifying HR's Role in Compliance Systems

Read the situation below:

A Ukrainian energy company is revising its HR policies after an internal audit revealed weak links between employee evaluations and compliance training.

The HR director plans to introduce new procedures for recruitment, onboarding, and competence assessment aligned with ISO 37303:2025.

Tasks:

> Identify which HR processes directly affect compliance performance.
> Propose how recruitment, onboarding, and training programs could embed ethical-behaviour criteria.
> Suggest two measurable indicators (KPIs) to evaluate HR compliance effectiveness.

Note: When formulating your answers, refer to the principles of ISO 37303:2025 and relevant Ukrainian legislation (e.g., Labour Code, Law "On Prevention of Corruption," Law "On Ensuring Equal Rights and Opportunities for Women and Men").

Exercise 2 – Developing a Competence Framework

Your team acts as consultants for a manufacturing firm preparing for ISO 37303 certification.

Tasks:

> Define three key compliance competences for middle managers (knowledge, skills, and attitudes).

> Design a short competence-assessment checklist suitable for annual reviews.

> Explain how this framework supports both compliance assurance and employee motivation.

Exercise 3 – Designing a Continuous Professional Development (CPD) Plan

Develop a CPD plan for compliance officers in a public organization.

Tasks:

> Outline annual CPD goals linked to organizational risk areas.
> Propose at least three training formats (e-learning, workshops, mentoring, etc.).
> Describe how CPD outcomes should be measured and reported to management.

Note: Align your plan with the ISO 37303:2025 "Compliance Management Systems — Guidelines for Competence and Training" and the Ukrainian Law "On Professional Development of Employees", ensuring conformity with national anti-corruption and labour standards.

Exercise 4 – Evaluating Ethical Performance

Tasks:

- > Suggest how ethical behaviour and compliance participation can be integrated into performance-evaluation forms.
- > Provide an example of an “ethical KPI.”
- > Discuss how managers can avoid bias when assessing ethical conduct.

Exercise 5 – Designing a Compliance Training Module

Imagine you are part of the HR–Compliance team at a logistics company implementing anti-corruption training.

Tasks:

- > Define the learning objectives of a short (1-hour) awareness session.
- > Choose appropriate delivery methods (e-learning, gamification, simulations, etc.).
- > Suggest how to evaluate both knowledge retention and behavioural change.
- > Explain how the module aligns with ISO 37303 and national anti-corruption legislation.

Exercise 6 – Building HSEQ Culture

Scenario: A construction company has strong safety rules but weak employee engagement. Accidents still occur due to “routine shortcuts.”

Tasks:

- > Identify cultural barriers affecting safety behaviour.
- > Propose initiatives to promote “zero-harm” and ethical responsibility.
- > Suggest how leadership and communication can reinforce HSEQ values.

Exercise 7 – Designing a Whistleblowing Mechanism

Following ISO 37002:2021 guidelines and Ukrainian legislation (Law “On Prevention of Corruption,” Art. 53–53⁴):

Tasks:

- > Develop a simple structure for an internal whistleblowing policy (reporting channels, confidentiality, protection, feedback).
- > Explain how HR should train employees to use the system without fear.
- > Describe how trust and psychological safety can be measured.

Exercise 8 – Applying HR Compliance Analytics

Scenario: Your company uses an HR analytics dashboard (SAP SuccessFactors) that tracks training participation, overtime, and risk indicators.

Tasks:

> Identify two compliance risks that can be detected through data analytics.

> Propose ethical safeguards to prevent misuse of employee data.

> Explain how predictive analytics can support early-risk prevention while maintaining privacy.

Exercise 9 – Ethical Leadership Simulation

Scenario: An HR manager discovers that an AI-based recruitment tool favours certain demographic groups. The CEO wants fast results and minimal disruption.

Tasks:

> Identify the ethical dilemma and key stakeholders.

> Apply the principles of responsible and ethical leadership to propose an action plan.

> Discuss how to communicate this issue transparently within the company.

Exercise 10 – Integrated Compliance Scenario

Team project integrating all sections of Chapter 6.

Scenario: Your group acts as a compliance task force for a Ukrainian enterprise preparing for ISO 37303 certification. The company must improve HR compliance systems, training, competence, HSEQ culture, and digital transparency.

Tasks:

> Map out key areas for improvement using Chapter 6 concepts.

> Develop a short “Compliance Action Roadmap” including objectives, responsible departments, and performance indicators.

> Present your roadmap as a policy briefing or poster demonstrating the link between HR, ethics, and sustainable corporate governance.

Target Questions

1. How does Human Resource Management (HRM) contribute to building and maintaining an effective compliance system within an organization?
2. In what ways can recruitment and onboarding processes influence the development of ethical culture and compliance awareness among new employees?
3. What are the main principles of integrating compliance requirements into HR

policies and procedures according to ISO 37303:2025?

4. How does competence management, in line with ISO 37303:2025, support risk-based compliance, and why is Continuous Professional Development (CPD) essential for maintaining ethical competence in changing regulatory environments?
5. What are the key differences between traditional performance appraisal and compliance-oriented evaluation systems?
6. How can HR departments measure and promote ethical behaviour using Key Performance Indicators (KPIs) that reflect integrity, HSEQ culture, and compliance effectiveness?
7. Why is compliance training considered both an educational and a cultural process?
8. What are the main components of an ethical HSEQ (Health, Safety, Environment, and Quality) culture, and how do they reinforce integrity, trust, and employee engagement in compliance systems?
9. How do whistleblowing mechanisms enhance transparency and trust inside organizations? What elements ensure their credibility, confidentiality, and protection of employees?
10. In what ways do digital transformation and HR compliance analytics change how organizations detect, prevent, and manage ethical risks?
11. What ethical and legal challenges arise from the use of artificial intelligence and predictive analytics in HR decision-making, and how can leaders ensure responsible AI practices in line with the EU AI Act (2024) and ISO 37303:2025?
12. How does ethical leadership influence compliance behaviour and organizational culture in the digital era?
13. What competences should future HR-compliance leaders possess to balance technological innovation with human-centred ethical values and resilience?
14. How can Ukrainian enterprises and public institutions align their HR-compliance systems with European standards (ISO 37303, ISO 37000, CSRD, and the EU AI Act) while considering national legal frameworks and institutional capacity?
15. How integrating ESG principles, ethical leadership, and HR compliance contributes to long-term organizational sustainability and stakeholder trust.

References for Self-study

1. ArcelorMittal Kryvyi Rih. (n.d.). *Ecology: Environmental management.* https://ukraine.arcelormittal.com/en/ecology
2. Armstrong, M., & Taylor, S. (2021). *Armstrong's handbook of human resource management practice* (16th ed.). Kogan Page. https://www.koganpage.com/hr-learning-development/armstrong-s-handbook-of-human-resource-management-practice-9781398606630

3. Becker, B. E., & Gerhart, B. (1996). The impact of human resource management on organizational performance. *Academy of Management Journal, 59*(2), 779–801. https://doi.org/10.2307/256712

4. Becker, B. E., & Gerhart, B. (2016). The impact of human resource management on organizational performance: Progress and prospects. *Academy of Management Journal, 39*(4), 779–801. https://doi.org/10.2307/256712

5. Boyatzis, R. E. (2009). Competencies as a behavioral approach to emotional intelligence. *Journal of Management Development, 28*(9), 749–770. https://doi.org/10.1108/02621710910987647

6. Branch, W. T., Jr., & George, M. (2017). Reflection-based learning for professional ethical formation. *AMA Journal of Ethics, 19*(4), 349–356. https://doi.org/10.1001/journalofethics.2017.19.4.medu1-1704

7. Brown, M. E., Treviño, L. K., & Harrison, D. A. (2005). Ethical leadership: A social learning perspective for construct development and testing. *Organizational Behavior and Human Decision Processes, 97*(2), 117–134. https://doi.org/10.1016/j.obhdp.2005.03.002

8. Butterfield, K. D., Treviño, L. K., & Weaver, G. R. (2000). Moral awareness in business organizations: Influences of issue-related and social context factors. *Human Relations, 53*(7), 981–1018. https://doi.org/10.1177/0018726700537004

9. Christian, M. S., Bradley, J. C., Wallace, J. C., & Burke, M. J. (2009). Workplace safety: A meta-analysis of the roles of person and situation factors. *Journal of Applied Psychology, 94*(5), 1103–1127. https://doi.org/10.1037/a0016172

10. Clarke, S. (2006). The relationship between safety climate and safety performance: A meta-analytic review. *Journal of Occupational Health Psychology, 11*(4), 315–327. https://doi.org/10.1037/1076-8998.11.4.315

11. Clarke, T. (2021). *Corporate governance: A survey.* Cambridge University Press. https://doi.org/10.1017/9781108966719

12. Decree of the President of Ukraine No. 225/2021 of June 2, 2021 On the Human Development Strategy. https://zakon.rada.gov.ua/laws/show/225/2021

13. Deloitte. (n.d.). *Ethics: Global principles of business conduct.* https://www.deloitte.com/tz/en/about/story/purpose-values/ethics.html

14. DTEK. (2024). *Compliance program 2024–2026.* https://dtek.com/content/upload/documents/compliance-programme-2024-2026.pdf

15. European Commission. (2020). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: European skills agenda for sustainable competitiveness, social fairness and resilience.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0274

16. European Union. (2000). *Directive 2000/78/EC establishing a general framework for equal treatment in employment and occupation.* https://eur-lex.europa.eu/eli/dir/2000/78/oj/eng

17. European Union. (2016). *Regulation (EU) 2016/679 ... (General Data Protection Regulation).* https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

18. European Union. (2019). *Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law (Whistleblower Protection Directive).* https://eur-lex.europa.eu/eli/dir/2019/1937/oj/eng

19. European Union. (2022). *Directive (EU) 2022/2464 ... as regards corporate sustainability reporting.* http://data.europa.eu/eli/dir/2022/2464/oj

20. European Union. (2024). *Regulation (EU) 2024/1689 ... (Artificial Intelligence Act). Official Journal of the European Union, L 168/1.* https://eur-lex.europa.eu/eli/reg/2024/1689/oj

21. Europass. (n.d.). *The European Qualifications Framework (EQF).* https://europass.europa.eu/en/european-qualifications-framework-eqf

22. Friedman, A. L. (2023). Continuing professional development as lifelong learning and education. *International Journal of Lifelong Education, 42*(6), 588–602. https://doi.org/10.1080/02601370.2023.2267770

23. Garavan, T., McCarthy, A., Sheehan, M., Lai, Y., Saunders, M., Clarke, N., Carbery, R., & Shanahan, V. (2019). Measuring the organizational impact of training: The need for greater methodological rigor. *Human Resource Development Quarterly, 30*(3), 291–309. https://doi.org/10.1002/hrdq.21345

24. Greenwood, M. R. (2002). Ethics and HRM: A review and conceptual analysis. *Journal of Business Ethics, 36*(3), 261–278. https://doi.org/10.1023/A:1014090411946

25. International Labour Organization. (1981). *C155 – Occupational Safety and Health Convention, 1981 (No. 155).* https://www.ilo.org/resource/c155-occupational-safety-and-health-convention-1981-no-155

26. International Labour Organization. (2006). *C187 – Promotional Framework for Occupational Safety and Health Convention, 2006 (No. 187).* https://www.ilo.org/resource/c187-promotional-framework-occupational-safety-and-health-convention-2006

27. International Labour Organization. (2024). *Safety and health at work.* International Labour Office. https://www.ilo.org/topics-and-sectors/safety-and-health-work

28. International Organization for Standardization. (2015). *Environmental management systems—Requirements with guidance for use (ISO Standard No. 14001:2015).* https://www.iso.org/standard/60857.html

29. International Organization for Standardization. (2015). *Quality management systems—Requirements (ISO Standard No. 9001:2015).* https://www.iso.org/standard/62085.html

30. International Organization for Standardization. (2018). *Occupational health and safety management systems—Requirements with guidance for use (ISO Standard No. 45001:2018).* https://www.iso.org/standard/63787.html

31. International Organization for Standardization. (2021). *Compliance management*

systems—Requirements with guidance for use (ISO Standard No. 37301:2021). https://www.iso.org/standard/75080.html

32. International Organization for Standardization. (2021). *Governance of organizations—Guidance (ISO Standard No. 37000:2021).* https://www.iso.org/standard/65036.html
33. International Organization for Standardization. (2021). *Whistleblowing management systems—Guidelines (ISO Standard No. 37002:2021).* https://www.iso.org/standard/65035.html
34. International Organization for Standardization. (2025). *Compliance management systems—Guidance for competence management (ISO Standard No. 37303:2025).* https://www.iso.org/standard/37303
35. Kaptein, M. (2008). Developing and testing a measure for the ethical culture of organizations: The corporate ethical virtues model. *Journal of Organizational Behavior, 29*(7), 923–947. https://doi.org/10.1002/job.520
36. Kaptein, M. (2015). The effectiveness of ethics programs: The role of scope, composition, and sequence. *Journal of Business Ethics, 132*(2), 415–431. https://doi.org/10.1007/s10551-014-2296-3
37. Knode, R. L. (2020). A new way of looking at safety culture maturity models: The lens of employee engagement. *Society of Petroleum Engineers.* https://doi.org/10.2118/201259-MS
38. Labour Code of Ukraine (No. 322-VIII, December 10, 1971). https://zakon.rada.gov.ua/laws/show/322-08
39. Law of Ukraine On Civil Service (No. 889-VIII, December 10, 2015). https://zakon.rada.gov.ua/laws/show/889-19
40. Law of Ukraine On Electronic Identification and Electronic Trust Services (No. 2155-VIII, October 5, 2017). https://zakon.rada.gov.ua/laws/show/2155-19
41. Law of Ukraine On Environmental Protection (No. 1264-XII, June 25, 1991). https://zakon.rada.gov.ua/laws/show/1264-12
42. Law of Ukraine On Ensuring Equal Rights and Opportunities for Women and Men (No. 2866-IV, August 8, 2005). https://zakon.rada.gov.ua/laws/show/2866-15
43. Law of Ukraine On Labour Protection (No. 2694-XII, October 14, 1992). https://zakon.rada.gov.ua/laws/show/2694-12
44. Law of Ukraine On Prevention of Corruption (No. 1700-VII, October 14, 2014). https://zakon.rada.gov.ua/laws/show/1700-18
45. Law of Ukraine On Professional Development of Employees (No. 4312-VI, January 12, 2012). https://zakon.rada.gov.ua/laws/show/4312-17
46. Law of Ukraine On Technical Regulations and Conformity Assessment (No. 124-VIII, January 15, 2015). https://zakon.rada.gov.ua/laws/show/124-19
47. Microsoft. (n.d.). *Corporate responsibility: Global human rights and responsible business conduct report.* https://www.microsoft.com/en-us/corporate-

responsibility/human-rights

48. Ministry of Digital Transformation of Ukraine. (2024). *Technologies: Regulation of artificial intelligence in Ukraine — presenting the White Paper.* https://thedigital.gov.ua/news/technologies/regulyuvannya-shtuchnogo-intelektu-v-ukraini-prezentuemo-bilu-knigu
49. NAVEX Global. (2025). *Whistleblowing and incident management benchmark report.* NAVEX Global. https://cdn.navex.com/image/upload/v1742410133/resources-2025/benchmarking-reports/2025-navex-whistleblowing-incident-mgt-benchmark-report.pdf
50. Naftogaz Group. (n.d.). *Ethics and compliance: Sustainability.* https://www.naftogaz.com/en/policies
51. Naftogaz Group. (n.d.). *Naftogaz launches the Trust Line in a new format.* https://www.naftogaz.com/news/trust-line-new-format
52. National Agency on Corruption Prevention (NAZK). (2023, September 6). *Launch of the unified whistleblowing portal.* https://nazk.gov.ua/uk/novyny/6-veresnya-nazk-zapuskaye-yedynyj-portal-povidomlen-vykryvachiv
53. Order of the Cabinet of Ministers of Ukraine No. 1351-r of December 31, 2024 On the Strategy for Digital Development of Innovative Activity of Ukraine until 2030. https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80
54. Order of the National Agency on Corruption Prevention (NACP) No. 127/20 of April 2, 2020 On Approval of the Requirements for the Protection of Anonymous Communication Channels for Reporting Possible Facts of Corruption or Corruption-Related Offences. https://zakon.rada.gov.ua/laws/show/z0370-20
55. Organisation for Economic Co-operation and Development. (2016). *Committing to effective whistleblower protection.* OECD Publishing. https://doi.org/10.1787/9789264252639-en
56. Organisation for Economic Co-operation and Development. (2023). *OECD guidelines for multinational enterprises on responsible business conduct.* OECD Publishing. https://www.oecd.org/en/publications/oecd-guidelines-for-multinational-enterprises-on-responsible-business-conduct_81f92357-en.html
57. Paine, L. S. (1994). Managing for organizational integrity. *Harvard Business Review, 72*(2), 106–117. https://hbr.org/1994/03/managing-for-organizational-integrity
58. Reason, J. (1997). *Managing the risks of organizational accidents* (1st ed.). Routledge. https://doi.org/10.4324/9781315543543
59. Rousseau, D. M. (1995). *Psychological contracts in organizations: Understanding written and unwritten agreements.* SAGE Publications. https://doi.org/10.4135/9781452231594
60. SAP. (n.d.). *Ethical usage of AI in the recruiting process. SAP Careers.* Retrieved November 2, 2025, from https://jobs.sap.com/content/Ethical_usage_of_AI_in_the_recruiting_process/?locale=en_US

61. SAP News. (2021, February). *Naftogaz Group adopts SAP S/4HANA to drive digital transformation.* https://news.sap.com/ukraine/2021/02/naftogaz-s4hana

62. Schein, E. H. (2010). *Organizational culture and leadership* (4th ed.). Jossey-Bass. https://ia800805.us.archive.org/9/items/EdgarHScheinOrganizationalCultureAndLeadership/Edgar_H_Schein_Organizational_culture_and_leadership.pdf

63. Shell. (2023). *Sustainability report 2023.* https://www.shell.com/sustainability/reporting-centre/reporting-centre-archive.html

64. Shiri, R., El-Metwally, A., Sallinen, M., Pöyry, M., Härmä, M., & Toppinen-Tanner, S. (2023). The role of continuing professional training or development in maintaining current employment: A systematic review. *Healthcare, 11*(21), 2900. https://doi.org/10.3390/healthcare11212900

65. Siemens. (n.d.). *Company: Compliance.* https://www.siemens.com/global/en/company/sustainability/compliance.html

66. Siemens. (2023). *Siemens sustainability report 2023.* https://assets.new.siemens.com/siemens/assets/api/uuid:00095b96-4712-4cd1-b045-19d5df704358/sustainability-report-fy2023.pdf

67. Siemens Energy. (n.d.). *Reporting channels "Speak Up" and Ombudsperson.* https://www.siemens-energy.com/global/en/home/company/compliance/reporting-channels.html

68. Sims, R. R. (2002). Business ethics teaching for effective learning. *Teaching Business Ethics, 6*(4), 393–410. https://doi.org/10.1023/A:1021107728568

69. Treviño, L. K., & Nelson, K. A. (2021). *Managing business ethics: Straight talk about how to do it right* (8th ed.). John Wiley & Sons. https://www.yourhomeworksolutions.com/wp-content/uploads/edd/2020/03/managing_business_ethics_straight_talk_about_how_to_do_it_right__7th_edition__linda_k._trevino.pdf

70. Treviño, L. K., Weaver, G. R., & Brown, M. E. (2008). It's lovely at the top: Hierarchical levels, identities, and perceptions of organizational ethics. *Business Ethics Quarterly, 18*(2), 233–252. https://doi.org/10.1017/S1052150X00010952

71. Ukrenergo. (n.d.-a). *Charter, constituent documents, codes, policies: Codes and policies.* https://ua.energy/about_us/charter/codes-and-policies/

72. Ukrenergo. (n.d.-b). *Code of ethics.* https://ua.energy/about_us/compliance/code-of-ethics/

73. Unilever. (n.d.). *Responsible business: Business integrity.* https://www.unilever.com/sustainability/responsible-business/business-integrity/

74. Weaver, G. R., & Treviño, L. K. (2001). The role of human resources in ethics/compliance management: A fairness perspective. *Human Resource Management Review, 11*(1–2), 113–134. https://doi.org/10.1016/S1053-4822(00)00043-7

1. *Essay: The Role of HR in Building a Compliance Culture (2 pages).* Analyze how HR policies on recruitment, training, and appraisal contribute to compliance awareness and ethical behavior in organizations.
2. *Mini-Case Study: Ethical Leadership and HSEQ (3–4 pages).* Choose a Ukrainian or international company (e.g., Siemens, Ukrenergo, Naftogaz). Identify how leadership decisions have shaped its HSEQ and compliance culture. Discuss what practices could be adapted for Ukrainian enterprises.
3. *Comparative Table: HR Compliance vs ESG Compliance.* Compare EU and Ukrainian approaches to integrating HR and compliance requirements into ESG and sustainability frameworks. Highlight key gaps and provide improvement recommendations.
4. *Interview Assignment: Human-Centric Compliance.* Conduct an interview with an HR manager or compliance officer. Summarize key insights on maintaining integrity, employee trust, and psychological safety within compliance systems (1 page reflection).
5. *Practical Task: Designing a Compliance Training Program*. Propose a short employee training or awareness program (2 pages) that supports ISO 37303 and ISO 45001 principles, focusing on ethical leadership and risk awareness.
6. *Applied Research: National HR-Compliance Framework*. Select one Ukrainian law (e.g., “On Labour Protection,” “On Prevention of Corruption”). Summarize compliance obligations for employers and HR departments and compare them with relevant EU directives.

Chapter 7: Compliance Communication and Whistlblowing

Learning Outcomes

After studying this chapter, learners will be able to:

- Explain how clear compliance communication supports a safe *Speak Up / Listen Up* culture and why it is essential for early detection of risks.
- Identify the main whistleblowing options (internal, external, public) and understand identity modes (open, confidential, anonymous) together with key safeguards such as confidentiality, non-retaliation, and expected timelines.
- Evaluate whether a reporting system works effectively by looking at basic indicators (timely acknowledgement, feedback, protection measures, lessons learned) and propose improvements where needed.

Key Words: whistleblowing, whistlblower, whistleblowing management system, wrongdoing, reporting channels, confidentiality, anonymity, non-retaliation, detrimental conduct

Main Definitions

Wrongdoing - action(s) or omission(s) that can cause harm.

Whistleblowing - reporting of wrongdoing by a whistleblower who has reasonable grounds to believe that the information reported is true at the time of reporting.

*Whistleblowing management functio*n - person(s) with responsibility and authority for the operation of the whistleblowing *management system.*

Triage - assessment of the initial report of wrongdoing for the purposes of categorization, taking preliminary measures, prioritization and allocation.

Detrimental conduct - any threatened, proposed or actual, direct or indirect, act or omission that can result in harm to a whistleblower or other relevant party, related to the reporting of wrongdoing.

Protected disclosure – a report of wrongdoing that meets the requirements set out in applicable law or internal policy and entitles the whistleblower to protection against any form of detrimental conduct.

Retaliation – a form of detrimental conduct involving any unfair or adverse treatment (such as dismissal, demotion, mobbing, or harassment) that occurs as a result of reporting wrongdoing.

Impartiality – a principle requiring that persons involved in the assessment, handling, or investigation of a report act objectively and remain free from conflicts of interest.

Standards, Laws, and Regulations

1. International: ISO 37002:2021 Whistleblowing management systems – Guidelines;

ISO 37301:2021 Compliance management systems - Requirements with guidance for use; ISO 37303:2025 Compliance management systems - Guidance for competence management; ISO 31000:2018 Risk management – Guidelines; ISO 45001:2018 Occupational health and safety management systems - Requirements with guidance for use; ISO 9001:2015 Quality management systems – Requirements; ISO 14001:2015 Environmental management systems - Requirements with guidance for use

2. European Union (EU): Directive 2000/78/EC of 27 November 2000 Establishing a general framework for equal treatment in employment and occupation*;* Regulation (EU) 2016/679 of 27 April 2016 General Data Protection Regulation (GDPR) — On the protection of natural persons with regard to the processing of personal data; Directive (EU) 2019/1937 of 23 October 2019 On the protection of persons who report breaches of Union law (Whistleblowing Directive); Directive (EU) 2022/2464 of 14 December 2022 Corporate Sustainability Reporting Directive (CSRD)

3. Ukraine: Labour Code of Ukraine; Law of Ukraine “On Prevention of Corruption”; Law of Ukraine “On Occupational Safety”; Law of Ukraine “On Ensuring Equal Rights and Opportunities for Women and Men”; Law of Ukraine “On Professional Development of Employees”; Order of the National Agency on Corruption Prevention (NACP) No. 127/20 of April 2, 2020 “On Approval of the Requirements for the Protection of Anonymous Communication Channels for Reporting Possible Facts of Corruption or Corruption-Related Offences”

List of Subchapters

7.1 Ethical and Organizational Role of Whistleblowing

7.2 International and European Standards on Whistleblowing. Ukrainian legislation

7.3 The Role and Status of Whistleblowers

7.4. Whistleblowing Management System

7.5 Building Trust and Psychological Safety. Integration with HR, Audit, and Compliance Governance

7.6 Challenges and Future Directions in Promoting Wistlblowing

7.1 Ethical and Organizational Role of Whistleblowing

Whistleblowing is a fundamental element of an organization’s ethical and compliance framework, reflecting its level of trust, openness, and accountability. It enables employees and stakeholders to report suspected violations - such as corruption, fraud, safety breaches, or human rights abuses - without fear of retaliation or discrimination. A healthy reporting culture signals transparency and ethical maturity, while the absence of open communication often indicates systemic weaknesses. Therefore, whistleblowing should not be viewed merely as a procedural compliance mechanism but as a moral and organizational commitment to justice, fairness, and responsibility that sustains long-term trust between management, employees, and society.

According to B. Culiberg and K. Mihelič (2017), whistleblowing constitutes both a moral and organizational process grounded in employees' perceptions of fairness, trust, and responsibility. The authors emphasize that organizations promoting transparency, justice, and ethical dialogue are more likely to encourage employees to disclose wrongdoing, transforming reporting from an act of risk into a manifestation of integrity.

Building on this, H. Park and J. Blenkinsopp (2009) conceptualize whistleblowing as a planned behavioral act shaped by moral obligation, perceived organizational support, and confidence that reported issues will be addressed justly. Their findings show that ethical leadership and procedural fairness significantly increase employees' willingness to report misconduct.

Complementing these perspectives, A. Jones (2015) argues that whistleblowing systems should function as learning mechanisms within an organizational culture, enabling improvement and accountability rather than punishment. A supportive "speak-up" environment fosters trust and shared responsibility, allowing employees to view reporting not as defiance but as constructive participation in ethical governance.

Collectively, these studies reveal that effective whistleblowing mechanisms can flourish only in organizations with cultures rooted in fairness, ethical leadership, and transparent communication - where speaking up is regarded as a positive contribution to integrity and continuous learning.

The terms "speak up" an**d** "raise a concern" are often used to make reporting feel more accessible and less intimidating. "Speak up" is an invitation for employees to share concerns, questions, or risks, while "raise a concern" refers to submitting an issue through an official reporting channel. These phrases help reduce stigma, encourage earlier communication, and support psychological safety. However, "whistleblowing" remains the formal legal term for protected disclosures.

A real speak-up culture is only possible when the organisation also knows how **to** listen and act**.** This is where the "listen up" concept becomes essential. It refers to organisational behaviours that ensure reports are taken seriously, handled confidentially, investigated fairly, and closed with proper feedback. In practice, this means that employees are encouraged to speak up and the organisation commits to listening, protecting, and responding responsibly.

7.2 International and European Standards on Whistleblowing. Ukrainian legislation

Global and European standards provide the foundation for transparent, fair, and secure whistleblowing practices that safeguard individuals and strengthen organizational integrity:

- Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law - establishes a unified framework for whistleblower protection within the EU. It defines internal, external, and public disclosure channels and obliges Member

States to ensure protection against retaliation and guarantee confidentiality.

- ISO 37002:2021 Whistleblowing management systems - Guidelines - provides internationally recognized principles and guidance for establishing, implementing, operating, maintaining, and continually improving effective whistleblowing management systems that promote trust, impartiality, and protection.
- ISO 37303:2025 Compliance management systems - Guidance for competence management complements ISO 37301:2021 (Compliance management systems - Requirements with guidance for use) by defining the competence, ethical awareness, and communication capabilities necessary for the effective functioning of compliance and integrity systems.

There is no law on whistleblowing in Ukraine. But the whistleblowing framework has been progressively harmonized with European and international standards through legal and institutional reforms:

- Law “On Prevention of Corruption” defines the legal status of whistleblowers, guarantees anonymity, and provides legal and financial protection mechanisms.
- Order of the National Agency on Corruption Prevention (NACP) No. 127/20 of April 2, 2020 “On Approval of the Requirements for the Protection of Anonymous Communication Channels for Reporting Possible Facts of Corruption or Corruption-Related Offences” establishes detailed procedural and technical requirements for creating and maintaining secure internal and external reporting channels within organizations, ensuring confidentiality and data protection.

Collectively, these frameworks institutionalize whistleblowing as a protected civic and ethical act, embedding it within systems of good governance, transparency, and accountability at both the international and national levels.

In 2019, the European Union adopted the “Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law” (Whistleblower Protection Directive). The Directive requires the creation of secure channels for complaints within organizations – private or public – and to public authorities. It also provides whistleblowers with a high level of protection against retaliation, and national authorities will need to adequately inform citizens of the requirements and provide training to public officials on how to deal with complaints. Those protected by the new rules include anyone who could acquire information on breaches in a work-related context. e.g. employees, including civil servants at national/local level, volunteers and trainees, non-executive members and shareholders.

The main requirements of Directive 2019/1937include: the creation of internal whistleblowing channels in companies with more than 50 workers; establishing a reporting channel hierarchy, with whistleblowers encouraged to use their organization’s internal channels before resorting to external channels that public authorities will have to create; whistleblower support and protection measures; and an obligation to provide information to authorities and companies.

The EU Whistleblowing Monitor https://whistleblowingmonitor.eu/ tracks how EU countries are putting whistleblower protection laws into practice.

In Ukraine there is a dedicated national platform called the Unified Whistleblower Reporting Portal https://whistleblowers.nazk.gov.ua/#/ . It allows individuals to submit reports about corruption, corruption-related offenses, or other violations of the Law of Ukraine "On Prevention of Corruption." The portal provides a secure channel for confidential or anonymous reporting and helps ensure that whistleblowers are protected while authorities receive timely and reliable information about potential misconduct.

ISO 37002:2001 Whistleblowing management systems - Guidelines provides guidelines for implementing, managing, evaluating, maintaining and improving a robust and effective management system within an organization for whistleblowing. ISO 37002 is flexible and can be adapted to a wide range of organizations, irrespective of size, sector, structure, geography, or jurisdiction. It is applicable to small, medium, and large organizations, as well as parts of an organization. In the private sector, ISO 37002 can be used by business enterprises as well as not-for-profit and non-governmental organizations. ISO 37002 can also be used in the public sector.

Additionally, ESG reporting frameworks, such as the Global Reporting Initiative and the Sustainability Accounting Standards Board, increasingly emphasize whistleblowing and corporate ethics as key indicators of governance and organizational integrity.

7.3 The Role and Status of Whistleblowers

Whistleblower - person who reports wrongdoing with the reasonable belief that the information reported was true at the time of reporting (ISO 37002:2001).

John K. Devitt (2015) emphasize that term whistleblowing was made popular in the early 70s by U.S. civic activist Ralph Nader to avoid the negative connotations of the words "informer" and "snitch". R. Nader defined whistleblowing as "an act of a man or woman who, believing that the public interest overrides the interest of the organization he serves, blows the whistle that the organization is [engaged] in corrupt, illegal, fraudulent or harmful activity". Nader's framing underscores that a whistleblower is not merely an employee **but** any person - inside or outside the organization - who, placing the public interest above organizational loyalty, reports corrupt, illegal, fraudulent, or harmful activity.

In Ukraine according to the Law of Ukraine on Prevention of Corruption a whistleblower is an individual that:

- has information about alleged corruption offenses – factual data, namely on the circumstances of the offense, the place and time of its commission and the person that committed the offense;
- is convinced in the accuracy of such information;
- received this information in the course of employment, professional, economic, social, scientific activities, service or training.

Wrongdoing means any action (e.g., active misconduct, bribery, unauthorized spending) or omission (e.g., failure to act, neglecting duties, concealing information) that causes, or could cause, harm to such protected interests: human rights, the environment, public health and safety, safe work-practices or the public interest.

Core forms of wrongdoing include:

- legal & ethical breaches: unethical behavior; fraud; corruption (including bribery); breach of national or international law; breach of the organizations or other applicable code of conduct.
- governance & compliance failures: gross negligence; breach of organization policy; abuse of authority; conflict of interest; gross waste or mismanagement.
- workplace misconduct: discrimination; bullying; harassment.
- financial/resources misuse: unauthorized use of public funds or resources; manipulation or misreporting that leads to waste or loss.

Potential harm may arise from a single event or a series of events (a pattern). From the view of time horizon wrongdoing or its harm may have occurred in the past, be ongoing, or be reasonably likely in the future. Therefore, classification of wrongdoing focuses on the risk or occurrence of harm, not only on formal rule violations.

Whistleblowing is the act of reporting suspected wrongdoing or risk of wrongdoing by a whistleblower who has reasonable grounds to believe that the information reported is true at the time of reporting.

Under Directive (EU) 2019/1937, whistleblowers must be protected from any form of retaliation, whether direct or indirect. Retaliation (detrimental conduct) refers to any negative consequence suffered because a person reported or disclosed wrongdoing. This protection applies not only to the whistleblower but also to people assisting them (colleagues, family members, facilitators).

The Directive (EU) 2019/1937 provides a non-exhaustive list of actions that qualify as retaliation (forms of detrimental conduct), including:

- Dismissal, suspension, or forced resignation.
- Demotion, withholding promotion, or changes to duties or responsibilities.
- Negative performance evaluation or disciplinary action based on the report.
- Harassment, intimidation, or discrimination at work.
- Damage to reputation, including online defamation or internal gossip.
- Blacklisting, hindering future employment or business opportunities.
- Withholding training, benefits, or professional development.
- Reduction of salary, working hours, or downgrading of working conditions.
- Transfer to less desirable roles, relocation, or change of workplace.
- Coercion, threats, or pressure from colleagues or management.

> Retaliation against third parties connected to the whistleblower (e.g., colleagues, relatives).

These examples reflect that retaliation is not limited to formal sanctions—it also includes subtle, informal, and psychological forms of pressure.

Directive (EU) 2019/1937 requires Member States and organisations to create robust anti-retaliation protections, including:

1. Prohibition of retaliation. Art. 19 explicitly prohibits all forms of detrimental conduct against whistleblowers acting in good faith.

2. Shift of burden of proof. If a whistleblower suffers harm, the organisation must prove that the action was not retaliation. This protects employees from being dismissed with pretextual reasons.

3. Confidentiality of identity. Art. 16 requires strict confidentiality of the whistleblower's identity and any identifying information. Protecting identity is one of the most effective ways to prevent retaliation.

4. Internal and external reporting channels. Art. 8–10 require organisations and authorities to set up secure, independent, and confidential channels. A well-designed system prevents leaks, misuse of information, and unauthorised access.

5. Support measures. Whistleblowers must have access to:

> independent advice and information,

> legal assistance,

> protective measures in labour disputes,

> financial and psychological support where necessary (Art. 20).

6. Clear procedures and timelines. Acknowledgement (7 days) and feedback (3 months) help maintain trust and reduce anxiety after reporting.

7.4 Whistleblowing Management System

Whistleblowing management system should be based on such principles (concepts) as:

> trust (employees and third parties can rely on the system to handle concerns fairly, securely, and on time);

> impartiality (reports are assessed and investigated objectively, free from conflicts of interest or undue influence);

> protection (people who report or participate (whistleblower, witnesses, implicated individuals) are protected from harm, including retaliation; sensitive data is safeguarded).

According to ISO 37002:2021, an effective whistleblowing system should uphold the following principles:

1. Accessibility - easy, multilingual access via secure digital or offline channels.
2. Confidentiality and anonymity - protection of identity and secure data processing under GDPR.
3. Protection from retaliation - legal and disciplinary safeguards.
4. Independence - oversight by an impartial compliance or ethics unit.
5. Transparency - feedback on actions taken and communication of lessons learned.
6. Training and awareness - continuous education to promote trust and reporting confidence.

L. Paine (1994) adds that trust is reinforced when organizations close the feedback loop addressing reports visibly and fairly.

Successful and responsive whistleblowing environment (ISO 37002) includes four pillows:

1) receiving reports;

2) assessing reports;

3) addressing reports;

4) concluding whistleblowing cases.

I. Receiving Reports. The ISO 37002 framework defines that a whistleblowing system should specify how reports can be made and received. In this framework, the organization is responsible for implementing secure, visible, and accessible reporting channels, with at least one channel connecting to a distinct authority outside of the management hierarchy. I. Receiving Reports: The ISO 37002 framework defines that a whistleblowing system should specify how reports can be made and received. In this framework, the organization is responsible for implementing secure, visible, and accessible reporting channels, with at least one channel connecting to a distinct authority outside of the management hierarchy.

Depending on whether and how the reporter's identity is revealed or protected, whistleblowing is categorized as:

> open whistleblowing: whistleblower discloses information without withholding their identity or requiring that their identity be kept secret.

> confidential whistleblowing: the identity and any information that can identify the whistleblower is known by the recipient but is not disclosed without the whistleblower's consent, unless required by legal and/or investigation process.

> anonymous whistleblowing: information is received without the whistleblower disclosing their identity.

The Directive (EU) 2019/1937 outlines three main channels for submitting reports: internal reporting, external reporting, and public disclosure. Each channel has its own requirements, safeguards, and conditions for protection.

1. Internal reporting. Internal channels must be established by private-sector entities with 50 or more employees (as well as certain regulated sectors regardless of size) and by public-sector entities, with limited exceptions for very small municipalities. These channels must be independent and secure, operated either in-house or by an external provider. Entities must designate an impartial person or department to follow up on reports and ensure two-way communication for requesting additional information and providing feedback. Reports may be submitted in writing or orally—such as through an online form, email, mail, telephone or voice messaging system—and in-person meetings must be offered within a reasonable timeframe. Organisations must acknowledge receipt within 7 days and provide feedback within 3 months, while ensuring strict confidentiality and secure record-keeping. Internal channels are the primary route, although this does not prevent individuals from using external mechanisms.

2. External reporting. External reporting channels must be provided by competent authorities designated by Member States. These channels must also be independent, autonomous, adequately resourced, and operated by trained staff. Authorities must ensure secure handling and durable storage of information to preserve confidentiality and integrity. Submission modes mirror internal channels: written or oral reporting, including online forms, email, telephone systems, and the option of an in-person meeting on request. Authorities must acknowledge reports within 7 days and provide feedback within 3 months, extendable to 6 months in justified cases. As with internal channels, strict confidentiality and secure record-keeping are required. Authorities must publish clear information online about how to report and what protections apply.

3. Public disclosure (to the media or the public). Public disclosure involves the whistleblower making information available directly to the public, for example, through the media or online. Protection under the Directive applies only if:

> the whistleblower first reported internally and/or externally and no appropriate action was taken within the required timelines, or

> the person has reasonable grounds to believe that there is an imminent or manifest danger to the public interest, a risk of retaliation, or a risk of evidence concealment or collusion.

Unlike internal and external channels, no timelines apply for public disclosure. Protection still requires that the report be made in good faith and within the scope of EU law covered by the Directive.

The Directive does not require entities or authorities to accept anonymous reports; this decision is left to Member States. However, if an anonymous whistleblower is later identified and suffers retaliation, they may still qualify for protection if other conditions are met.

II. Assessing Reports. The framework dictates that whistleblowing systems must have a clear and consistent process for assessing received reports. An organization's reporting process needs to ensure impartial assessment and management of reports. Additionally, any assessment-related decisions should be well-documented.

The process should include:

- Verifying whether the report falls within the scope of the whistleblowing procedure or should be redirected to other mechanisms (e.g. grievance, performance management, customer complaints).
- Conducting an initial plausibility check to confirm whether sufficient information is provided to proceed.
- Classifying the type of alleged wrongdoing (e.g. legal/ethical breach, governance failure, workplace misconduct, misuse of resources).
- Evaluating the potential risk or harm to human rights, public interest, health and safety, or the organisation's integrity.
- Determining the urgency of the matter, including whether immediate protective or preventive measures are required.
- Deciding whether the report should be handled internally, referred to a specialised function (e.g. compliance, internal audit, HR, health and safety), or escalated to external authorities.
- Ensuring confidentiality and safeguarding the whistleblower's identity throughout the process.
- Recording the assessment in a secure and auditable manner.

III. Addressing Reports. Under the ISO 37002 framework, the management of whistleblowing reports should be as efficient as possible while still addressing the full scope of the report. To accomplish this, all investigations must be adequately resourced, with clear terms of reference and well-defined and well-documented scope. When addressing whistleblowing reports, proper protections for whistleblowers and other relevant parties must be upheld.

The outcome of assessing the report may include doing one or more of the following:

- Engage with other functions (e.g. HR, legal, internal audit, compliance, health and safety, finance), if needed;
- Gather more information;
- Implement preliminary measures such as suspending the implicated person and securing evidence;
- Ensure that the whistleblower's safety and security are not compromised when his or her identity is known;
- Refer the whistleblower to other procedures such as the organization's grievance procedure; or
- Refer the case to relevant authorities such as law enforcement or regulatory bodies.

IV. Concluding Whistleblowing Cases. An effective whistleblowing system following the guidelines of ISO 37002 should have a clear mechanism for resolving and closing whistleblowing investigations. This resolution process must include steps for issuing

the investigation's findings, collecting relevant feedback, and identifying controls or policies in need of improvement to prevent similar future incidents.

Concluding a whistleblowing case may involve several actions such as:

> Issuing findings;

> Recommending remedial actions, sanctions, and changes to policies and procedures where control deficiencies were identified;

> Identifying lessons learnt;

> Providing feedback to the owner of the whistleblowing management system; and

> Providing feedback to the whistleblower and other relevant stakeholders about the findings of the investigation.

In order to maintain the effectiveness whistleblowing system should be formally reviewed at least annually, and revisions should be made accordingly to improve effectiveness and ensure systems are up to date and in line with legislation and best practice.

Case in Point: *Airbus (France). Airbus has established the OpenLine reporting channel, which enables employees and other stakeholders to submit concerns about possible misconduct securely and, where permissible, anonymously. The company emphasizes its commitment to a "Speak-Up" culture, protection of those who raise concerns in good faith, and fostering open dialogue across the organisation.*

Following the example of companies such as Airbus, it becomes evident that effective whistleblowing mechanisms rely not only on technical infrastructure but also on an environment of trust and mutual respect. The ability to speak up without fear reflects the maturity of an organisation's ethical culture and its commitment to fairness and transparency.

Organizations should designate an impartial person or department responsible for the operation whistleblowing system – whistleblower officer. This person or department should be free from conflict of interest, and have sufficient independence, powers and resources, as well as the relevant qualifications. Everyone in the organization has roles and responsibilities related to the design, planning, implementation, management, and ongoing maintenance of an ISO 37002 whistleblowing Management System. For example, leadership is responsible for supporting the program by prohibiting retaliation and ensuring sufficient resources are allocated to implement the programme. Management is responsible for implementing and managing the programme. All employees are responsible for knowing, and complying with, the whistleblowing policy, completing training, and reporting actual or potential cases of non-compliance.

Organisations should train managers and whistleblower officers in ethical behaviour, confidential handling, psychologically safe communication, and procedural competence, supported by scenario-based exercises. This ensures that reports are managed professionally, impartially, and in full compliance with the Whistleblowing Directive and ISO 37002, strengthening trust and integrity throughout the organisation.

Ukraine has made notable progress in establishing secure and ethical whistleblowing mechanisms in line with European standards.

In 2023, the National Agency on Corruption Prevention (NACP) launched the Unified Whistleblowing Portal, enabling public officials and citizens to report corruption-related offences confidentially or anonymously. The portal operates through an encrypted system, allows users to track the status of submitted reports, and provides educational materials to raise awareness about whistleblower rights and protections.

In addition, state-owned and corporate entities have started implementing internal reporting channels that promote integrity and transparency.

For example, in 2023, Naftogaz Group introduced its “Trust Line”, a confidential reporting channel managed by the compliance department. The system enables employees and partners to report potential violations, corruption risks, or unethical conduct while ensuring confidentiality and protection from retaliation.

The Ukrainian experience demonstrates that effective whistleblowing frameworks require not only regulatory compliance but also cultural transformation - where transparency, fairness, and open dialogue become embedded in everyday governance.

7.5 Building Trust and Psychological Safety. Integration with HR, Audit, and Compliance Governance

Such a system is essential to build trust in the organization and the organization’s commitment to ethical practices. Not only will such a system demonstrate leadership commitment to preventing and addressing wrongdoing, it will also encourage persons to report wrongdoing timeously, reduce and prevent unfavourable treatment and victimization of whistleblowers and other involved parties, encourage a culture of transparency and accountability, and ‘make it okay’ for people to blow the whistle.

Trust serves as the foundation of every whistleblowing system. Employees are more likely to report concerns when they are confident that their information will be treated fairly, confidentially, and without retaliation.

To strengthen this trust, organisations should:

- communicate clear commitments to non-retaliation and confidentiality;
- train managers to handle disclosures with empathy and professionalism;
- ensure visible leadership support that reinforces the importance of ethical communication;
- provide confidential counselling and accessible ethics hotlines;
- ecognise and encourage acts of ethical courage and responsibility.

Creating a psychologically safe environment transforms whistleblowing from a risky individual act into a shared organisational value — one that reinforces transparency, accountability, and long-term integrity.

Case in Point: *Deutsche Telekom (Germany). Deutsche Telekom operates its "Tell Me!" whistleblower portal, which enables employees and external stakeholders to report suspected violations of laws or internal policies, including anonymously. Confidentiality is guaranteed where legally permissible. The company publishes annual figures of incoming reports and emphasises its commitment to integrity, ethics and open communication.*

This example illustrates how a large multinational company integrates technical reporting channels with a culture of accountability, enabling transparency and reinforcing trust within its compliance system.

Building trust and psychological safety in whistleblowing systems lays the foundation for sustainable ethical behaviour within organisations. However, lasting impact can only be achieved when these mechanisms are not isolated initiatives but operate as an integral part of the organisation's overall governance and compliance framework.

To maximise their effectiveness, whistleblowing and ethics programmes should be systematically linked with human resource management, internal audit, and compliance processes, ensuring that lessons learned from reporting translate into continuous improvement, staff development, and policy enhancement.

Whistleblowing mechanisms therefore intersect directly with HR, audit, and compliance governance. The ISO 37303:2025 standard highlights the importance of integrating reporting data into broader organisational learning and improvement cycles. Practical applications include:

- linking trends in reported cases to staff training initiatives (e.g., data protection, anti-harassment, integrity awareness);
- analysing patterns to identify systemic risks and root causes;
- including whistleblowing metrics in performance and sustainability dashboards;
- using insights from reports to update policies, strengthen controls, and reinforce a culture of integrity and accountability.

When managed ethically and systematically, whistleblowing data becomes a valuable strategic resource that enables organisations to identify vulnerabilities, prevent risks, and strengthen their overall governance and ethical culture.

7.6 Challenges and Future Directions in Promoting Wistlblowing

Despite growing institutionalization and increased awareness, whistleblowing systems continue to face persistent challenges:

- fear of retaliation and social stigma, which discourages potential reporters;
- insufficient post-report communication, leading to diminished confidence in follow-up actions;
- procedural complexity, which can make reporting burdensome or unclear;

- limited awareness and training, particularly among employees in smaller organisations and the public sector.

At the same time, several emerging directions signal the future of whistleblowing management:

- the use of AI-supported detection and risk analytics, ensuring consistency with GDPR and ISO 37303 principles;
- adoption of blockchain-secured tracking systems to preserve data integrity and evidence authenticity;
- creation of cross-border reporting channels as part of EU–Ukraine legal and compliance integration;
- inclusion of whistleblowing KPIs in ESG and corporate compliance performance dashboards to enhance accountability and transparency.

By the end of this decade, trust and transparency in reporting systems are expected to become measurable dimensions of organizational reputation and ethical governance, influencing both stakeholder confidence and public legitimacy.

Practical Exercises

Exercise 1 – Identifying Elements of an Effective Whistleblowing System

Scenario:

A Ukrainian transport company is preparing to implement internal reporting channels after several incidents of unreported misconduct.

Tasks:

- Identify the key components of an internal whistleblowing system required by Directive (EU) 2019/1937 and ISO 37002:2021.
- Explain why confidentiality, impartiality, and non-retaliation are essential for system credibility.
- Suggest two organisational risks that arise when no reporting channel is available.

Exercise 2 – Categorising Reporting Channels

Scenario:

You are part of the ethics team advising a medium-sized IT company.

Tasks:

- Describe the differences between internal reporting, external reporting, and public disclosure under the Whistleblowing Directive.
- Provide an example of when each channel would be appropriate.

> Evaluate which channel should be prioritised within the company and why.

Exercise 3 – Designing a "Speak Up / Listen Up" Awareness Module

Tasks:

> Draft three key messages for a 30-minute internal training session that promotes a Speak Up culture.

> Define two Listen Up behaviours managers should demonstrate during report handling.

> Propose how to measure whether employees feel safe to report concerns.

Exercise 4 – Assessing Reports of Wrongdoing (Triage Exercise)

Scenario:

A whistleblower submits an anonymous report claiming procurement fraud but provides limited detail.

Tasks:

> Apply the steps of triage based on ISO 37002:2021 (scope check, plausibility, urgency, risk).

> Decide whether the case requires additional information, escalation, or referral to another function.

> Explain how confidentiality must be preserved even when the report lacks detail.

Exercise 5 – Evaluating Confidentiality and Data Protection

Scenario:

Your organisation uses a shared email inbox for receiving reports, and several employees have access.

Tasks:

> Identify confidentiality risks linked to this reporting method.

> Compare this approach with a secure digital platform aligned with NACP Order No. 127/20.

> Suggest technical and organisational measures to ensure data protection under GDPR and Ukrainian anti-corruption law.

Exercise 6 – Designing an Internal Reporting Policy

Tasks:

- Draft the basic structure of a whistleblowing policy, including channels, identity modes (open, confidential, anonymous), case-handling stages, timelines, and feedback.
- Explain how the policy should communicate protection against detrimental conduct.
- Recommend how the policy should be introduced to employees to ensure understanding and trust.

Exercise 7 – Analysing a Case of Retaliation

Scenario:

A procurement specialist is reassigned to a lower-responsibility role shortly after submitting a complaint.

Tasks:

- Identify whether this situation qualifies as detrimental conduct.
- Apply Directive (EU) 2019/1937 criteria to determine whistleblower protection.
- Propose remedial actions the organisation must take to prevent further retaliation.

Exercise 8 – Comparing Identity Modes: Open, Confidential, Anonymous

Tasks:

- Provide advantages and disadvantages of each identity mode for both the whistleblower and the organisation.
- Identify situations where anonymous reporting may be more appropriate than open reporting.
- Evaluate how organisations can maintain trust while allowing anonymity.

Exercise 9 – Leadership and Trust-Building in Whistleblowing Systems

Scenario:

Employee surveys show low confidence in management's handling of concerns.

Tasks:

- Identify leadership behaviours that strengthen employee trust in reporting systems.
- Propose three communication actions that demonstrate commitment to non-retaliation.
- Suggest how the organisation can measure psychological safety over time.

Exercise 10 – Integrated Whistleblowing Scenario (Final Project)

Scenario:

Your group acts as a task force responsible for designing a complete whistleblowing framework for a Ukrainian financial institution preparing for ISO 37002:2021 alignment.

Tasks:

> Map out system requirements: reporting channels, triage, investigation, feedback, protection, record-keeping, and roles (e.g., whistleblower officer).

> Develop a “Whistleblowing Implementation Roadmap” outlining phases, responsibilities, KPIs, and communication steps.

> Present your roadmap as a policy briefing, explaining how it supports transparency, ethical governance, and alignment with the Whistleblowing Directive and Ukrainian anti-corruption legislation.

Target Questions

1. What is whistleblowing, and how does it differ from general complaint mechanisms or internal grievance procedures?
2. How do communication practices influence the development of a functional Speak Up / Listen Up culture, and why are both elements necessary for credibility and trust?
3. What types of wrongdoing qualify for protected disclosure under ISO 37002:2021 and Directive (EU) 2019/1937, and why is it important to distinguish actions from omissions?
4. What are the main identity modes (open, confidential, anonymous), and how does each influence trust, investigation quality, and whistleblower protection?
5. How do internal, external, and public disclosure channels differ in terms of accessibility, protection, timelines, and conditions for legal protection?
6. What principles (trust, impartiality, protection) form the ethical foundation of an effective whistleblowing management system, and how do they shape organisational behaviour?
7. What steps are involved in receiving, assessing (triage), addressing, and concluding reports according to ISO 37002:2021?
8. What forms of detrimental conduct (retaliation) can whistleblowers face, and what legal and organisational measures are required to prevent and respond to such risks?
9. How should organisations train managers and whistleblower officers to respond ethically, confidentially, and professionally to concerns?

10. What challenges emerge when handling anonymous reports, and how can organisations ensure fairness and due process in such situations?
11. What role does leadership play in strengthening trust in reporting channels, ensuring non-retaliation, and modelling ethical communication?
12. What are the key differences between Ukraine's anti-corruption whistleblower provisions and the broader protection frameworks in the EU?

References for Self-study

1. Airbus. (n.d.). *Integrity and compliance.* https://www.airbus.com/en/sustainability/integrity-and-compliance
2. Culiberg, B., & Mihelič, K. K. (2017). The evolution of whistleblowing studies: A critical review and research agenda. *Journal of Business Ethics, 146*, 787–803. https://doi.org/10.1007/s10551-016-3237-0
3. Deutsche Telekom. (n.d.). *TellMe whistleblower portal.* https://www.telekom.com/en/company/compliance/details/tellme-whistleblower-portal-356032
4. Devitt, J. K. (2015). What is Whistleblowing? In: Speaking Up Safely Civil Society Guide to Whistleblowing: Middle East and North Africa Region. Transparency International, Jan.1, 5-7. http://www.jstor.org/stable/resrep20533.4
5. European Union. (2019). *Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law (Whistleblower Protection Directive).* https://eur-lex.europa.eu/eli/dir/2019/1937/oj/eng
6. Gramont, Jacqueline de (2017). The Business Case for "Speaking Up". How Internal Reporting Mechanisms Styrengthen Private-Sector Organisations. Transparency International. 16 p. https://www.transparency.org/en/publications/business-case-for-speaking-up
7. International Organization for Standardization. (2015). *Environmental management systems—Requirements with guidance for use (ISO Standard No. 14001:2015).* https://www.iso.org/standard/60857.html
8. International Organization for Standardization. (2015). *Quality management systems—Requirements (ISO Standard No. 9001:2015).* https://www.iso.org/standard/62085.html
9. International Organization for Standardization. (2018). *Occupational health and safety management systems—Requirements with guidance for use (ISO Standard No. 45001:2018).* https://www.iso.org/standard/63787.html
10. International Organization for Standardization. (2021). *Compliance management systems—Requirements with guidance for use (ISO Standard No. 37301:2021).* https://www.iso.org/standard/75080.html
11. International Organization for Standardization. (2021). *Governance of organizations—Guidance (ISO Standard No. 37000:2021).* https://www.iso.org/standard/65036.html

12. International Organization for Standardization. (2021). *Whistleblowing management systems—Guidelines (ISO Standard No. 37002:2021).* https://www.iso.org/standard/65035.html

13. International Organization for Standardization. (2025). *Compliance management systems—Guidance for competence management (ISO Standard No. 37303:2025).* https://www.iso.org/standard/37303

14. Jones, A. (2015). The role of employee whistleblowing and raising concerns in an organizational learning culture – elusive and laudable? *International Journal of Health Policy and Management, 5*(1), 67–69. https://doi.org/10.15171/ijhpm.2015.182

15. Labour Code of Ukraine (No. 322-VIII, December 10, 1971). https://zakon.rada.gov.ua/laws/show/322-08

16. Law of Ukraine On Civil Service (No. 889-VIII, December 10, 2015). https://zakon.rada.gov.ua/laws/show/889-19

17. Law of Ukraine On Electronic Identification and Electronic Trust Services (No. 2155-VIII, October 5, 2017). https://zakon.rada.gov.ua/laws/show/2155-19

18. Law of Ukraine On Ensuring Equal Rights and Opportunities for Women and Men (No. 2866-IV, August 8, 2005). https://zakon.rada.gov.ua/laws/show/2866-15

19. Law of Ukraine On Environmental Protection (No. 1264-XII, June 25, 1991). https://zakon.rada.gov.ua/laws/show/1264-12

20. Law of Ukraine On Labour Protection (No. 2694-XII, October 14, 1992). https://zakon.rada.gov.ua/laws/show/2694-12

21. Law of Ukraine On Prevention of Corruption (No. 1700-VII, October 14, 2014). https://zakon.rada.gov.ua/laws/show/1700-18

22. Maistrenko A., Nazarova K., Kopotiienko T., Ovcharuk R., Miniailo V., & Shalimova N. (2024). Anti-Corruption Audit of Companies and Foresight Analysis in Terms of the State`s European Integration Economic Policy. *Financial and Credit Activity Problems of Theory and Practice,* 6(59), 90-105. https://doi.org/10.55643/fcaptp.6.59.2024.4509

23. Naftogaz Group. (n.d.). *Naftogaz launches the Trust Line in a new format.* https://www.naftogaz.com/news/trust-line-new-format

24. National Agency on Corruption Prevention (NAZK). (2023, September 6). *Launch of the unified whistleblowing portal.* https://nazk.gov.ua/uk/novyny/6-veresnya-nazk-zapuskaye-yedynyj-portal-povidomlen-vykryvachiv

25. NAVEX Global. (2025). *Whistleblowing and incident management benchmark report.* NAVEX Global. https://cdn.navex.com/image/upload/v1742410133/resources-2025/benchmarking-reports/2025-navex-whistleblowing-incident-mgt-benchmark-report.pdf

26. Nowers, I. & Terracol, M. (2025). Monitoring Internal Whistleblowing Systems. A framework for collecting data and reporting on performance and impact.

Transparency International and Transparency International Ireland. 44 p. https://www.transparency.org/en/publications/monitoring-internal-whistleblowing-systems

27. Order of the Cabinet of Ministers of Ukraine No. 1351-r of December 31, 2024 On the Strategy for Digital Development of Innovative Activity of Ukraine until 2030. https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80
28. Order of the National Agency on Corruption Prevention (NACP) No. 127/20 of April 2, 2020 On Approval of the Requirements for the Protection of Anonymous Communication Channels for Reporting Possible Facts of Corruption or Corruption-Related Offences. https://zakon.rada.gov.ua/laws/show/z0370-20
29. Organisation for Economic Co-operation and Development. (2016). *Committing to effective whistleblower protection.* OECD Publishing. https://doi.org/10.1787/9789264252639-en
30. Paine, L. S. (1994). Managing for organizational integrity. *Harvard Business Review, 72*(2), 106–117. https://hbr.org/1994/03/managing-for-organizational-integrity
31. Park, H., & Blenkinsopp, J. (2009). Whistleblowing as planned behavior: A survey of South Korean police officers. *Journal of Business Ethics, 85*, 545–556. https://doi.org/10.1007/s10551-008-9788-y
32. Siemens Energy. (n.d.). *Reporting channels "Speak Up" and Ombudsperson.* https://www.siemens-energy.com/global/en/home/company/compliance/reporting-channels.html
33. Terracol, M. (2024), *Internal Whistleblowing Systems – Self-Assessment Framework for public and private organisations.* https://www.transparency.org/en/publications/internal-whistleblowing-systems-self-assessment-framework-public-private-organisations
34. Terracol, Marie (2022). Internal whistleblowing systems. Best practice principles for public and private organisations. Transparency International. 46 p. https://files.transparencycdn.org/images/2022_PolicyBrief_InternalWhistleblowingSystems_English-1.pdf

Assignments for Self-Study

1. *Essay:* The Role of Whistleblowing in Organizational Integrity (2 pages). Analyze how internal and external reporting channels contribute to transparency, ethical behaviour, and early detection of misconduct. Discuss why a Speak Up / Listen Up culture is essential for organisational trust and accountability.
2. *Mini-Case Study:* Whistleblowing and Organisational Response (3–4 pages). Choose a Ukrainian or international case of whistleblowing (e.g., Airbus, Deutsche Telekom, Danske Bank, Rebekah Jones). Identify how the organisation responded to the report of wrongdoing and evaluate whether its actions aligned with ISO 37002 and Directive (EU) 2019/1937. Propose which practices could be adapted for Ukrainian organisations.

3. *Comparative Table:* EU Whistleblowing Standards vs Ukrainian Anti-Corruption Framework. Compare requirements for reporting channels, identity protection, timelines, confidentiality, and retaliation safeguards in Directive (EU) 2019/1937 and the Law of Ukraine “On Prevention of Corruption”. Highlight key gaps and provide recommendations for harmonisation with European standards.

4. *Interview Assignment:* Trust and Psychological Safety in Reporting Systems (1 page reflection). Conduct an interview with a compliance officer, internal auditor, legal specialist, or HR manager. Summarize key insights on what encourages or discourages employees from reporting wrongdoing, how confidentiality is ensured, and how retaliation risks are managed.

5. *Practical Task:* Designing an Internal Whistleblowing Policy (2 pages). Develop a short policy that includes definitions, reporting channels, confidentiality rules, protection measures, investigation steps, and feedback requirements. Ensure the policy aligns with ISO 37002 and the Whistleblowing Directive’s minimum standards.

6. *Applied Research:* Legal and Procedural Requirements for Whistleblowing (2 pages). Select one regulatory framework (e.g., Directive (EU) 2019/1937, GDPR, NACP Order No. 127/20, Law “On Prevention of Corruption”). Summarize its obligations for organisations regarding reporting systems, confidentiality, and non-retaliation. Compare these requirements with ISO 37002 guidelines.

Chapter 8: Compliance Risk Management

Learning Outcomes

After studying this chapter, learners will be able to:

> Understand the methods of identifying, classifying, and assessing compliance risks.

> Acquire skills in identifying “red flags” and minimizing risks associated with third parties.

> Uderstand of modern technologies used in compliance and future trends (digital compliance, cybersecurity, blockchain).

Key words: compliance risk, compliance risk management system, compliance risk management process, approaches to assessing compliance risks, methods for assessing compliance risks, internal control mechanisms, technological solutions for managing compliance risks.

Main Definitions

Risk is an impact of uncertainty on the achievement of the objectives; influence is deviation from an expected outcome, which can be either positive or negative; uncertainty is a condition, even partial, of insufficient information, understanding or knowledge about an event, its consequences or the probability of it occurrence; risk often described in terms of potential “events” and “consequences”, or their combination; risk is often expressed as a combination of the consequences of an event (including changes in circumstances) and associated probability of its occurrence (ISO, 2021).

Compliance risk – the probability of losses/sanctions, additional losses or failure to receive planned income or loss of reputation as a result of non-compliance with the requirements of legislation, regulatory legal acts, market standards, rules of fair competition, rules of corporate ethics, the occurrence of a conflict of interest, as well as intra-bank/intra-group documents (Verkhovna Rada of Ukraine, 2018).

Risk management system – a set of properly documented and approved risk management policies, methodologies and procedures that define the course of action aimed at implementing a systematic process of identifying, measuring, monitoring, controlling, reporting and mitigating all types of risks at all organizational levels (Verkhovna Rada of Ukraine, 2018).

Standards, Laws, and Regulations

1. General: ISO 31000:2018 Risk management, ISO 37301:2021 Compliance management systems, Law of Ukraine «On Prevention of Corruption» dated 14.10.2014 № 1700-VII, ISO 37301:2021 Compliance management systems, Law of Ukraine “On Public Procurement” dated 25.12. 2015 № 922-VIII

2. Finance: NBU Regulation "On the Organization of Risk Management Systems in Ukrainian Banks" dated 11.06.2018 № 64, Law of Ukraine "On Capital Markets and Organized Commodity Markets" dated 23.02.2006 № 3480-IV

3. Education: Law of Ukraine "On Education" dated 05.09.2017 № 2145-VIII, Methodological recommendations on the application of tools and mechanisms for the transformation of various spheres of functioning of higher education institutions on the principles of transparency and integrity, approved by Order of the Ministry of Education and Science of Ukraine dated 17.04.2025 № 576

4. Manufacturing and services: Law of Ukraine "On Environmental Protection" dated 25.06.1991 № 1264-XII, ISO 14001:2015 Environmental management systems, ISO 45001:2018 "Occupational health and safety"

List of subsections

8.1 Theoretical and Practical Foundations of Compliance Risk Analysis

8.2 Compliance risk management system

8.3 Compliance risk management process

8.4 Tools and technologies

8.5 Compliance Risks and the Path Toward Sustainable Governance

8.1. Theoretical and Practical Foundations of Compliance Risk Analysis

In modern scientific discourse, compliance risk management is considered a key element of the effective functioning of financial and educational institutions. Sheludko S. A. and Yegorova A. S. revealed the essence of compliance and its place in bank risk management, emphasizing its role in ensuring regulatory compliance. Vodzianova V. analyzed the functional role of the risk management unit in monitoring the effectiveness of the bank's internal control system, which allows identifying and neutralizing potential violations. In the field of education, Tkachuk L. and Tkachuk M. have highlighted the specific features of managing an institution based on risk management principles, demonstrating the adaptation of financial approaches to the educational environment. As a whle, these studies form a multidimensional basis for the development of guidebooks that combine academic depth with practical value.

Compliance risk – the probability of occurrence and consequences of non-compliance with the obligations established by the organization in the field of compliance (ISO, 2021).

In particular, S. A. Sheludko and A. S. Yegorova note that the main factors of compliance risks are certain shortcomings in the organization of the bank's internal control system, and other important factors include the participation of bank employees in dubious transactions, their insufficient level of professional training; ineffective operation of the financial monitoring system and risk management (Sheludko & Yegorova, 2017).

In the context of modern economic transformation and the growing role of the regulatory environment, systematic research of compliance risks is gaining particular relevance. The feasibility of analyzing such risks in the context of individual sectors of the economy – financial, educational, production and service – is due to significant differences in the nature of legal regulation, the structure of operational activities, the level of digitalization and the specifics of interaction with internal and external stakeholders. Such a sectoral approach allows not only to identify typical areas of compliance vulnerability, but also to develop adaptive risk management mechanisms that correspond to industry specifics and contribute to the formation of sustainable, ethically oriented organizational practices (Table 8.1).

Table 8.1 Types of compliance risks by sectors of the economy

<table>
<tr><th>Manufacturing sector</th><th>Financial services sector</th><th>Education</th></tr>
<tr><td colspan="3">1. Regulatory and legal compliance risks.
2. Corruption and bribery.
3. Conflict of interest.
4. Violation of ethical norms and principles of business conduct.
5. Product compliance risk</td></tr>
<tr><td colspan="2">6. Interaction with counterparties</td><td>7. Violation of academic integrity</td></tr>
</table>

Source: Sheludko & Yegorova, 2017; Ministry of Education and Science of Ukraine, 2025

To better understand the unique nature of compliance risks, it is useful to compare them with other categories of risks such as financial, operational, and strategic. The following table highlights the key differences in their essence, sources of origin, management mechanisms, and potential consequences (Table 8.2).

.

Table 8.2 Difference between compliance risks and other types of risks (financial, operational, etc.)

Risk type	Essence	Source of origin	Management mechanism	Potential consequences
Financial	Loss of assets, profits, liquidity	Market fluctuations, currency changes, credit obligations	Hedging, reserves, diversification	Losses, bankruptcy, loss of investors

Opera-tional	Failures in processes, systems, human resources	Technical failures, staff errors, inefficient processes	Automation, audit, process optimization	Production stoppage, decrease in productivity
Strategic	Inconsistency with long-term goals	Uncertainty, errors during strategic planning	Scenario planning, SWOT / PESTLE analysis, external environment monitoring	Loss of market positions, financial losses, loss of trust from customers, partners and society
Complian-ce risk	Violation of norms, standards, ethical principles	Changes in legislation, non-compliance with policies, ethical violations	Codes of ethics, compliance programs, monitoring of regulatory changes	Fines, lawsuits, reputational damage, prohibition of activities

8.2. Compliance risk management system

The purpose of the compliance risk management system varies across different sectors of the economy. In the manufacturing sector, it is aimed at ensuring the stability of operations and increasing the efficiency of business processes through the implementation of compliance controls and the optimization of risk management procedures. Another important objective is strengthening the trust of counterparties by demonstrating high standards of corporate governance.

In the financial services sector, the system focuses on creating unified principles and approaches to the functioning of compliance risk management. This is directed toward maintaining a consistently high level of compliance risk management culture, which supports the integrity and sustainability of financial institutions.

Within the education sector, compliance risk management contributes to increasing management efficiency and reinforcing the reputation of higher education institutions. It also enhances the credibility of officials and employees, thereby promoting trust and ethical standards in the academic environment.

An effective compliance risk management system is typically structured according to the “three lines of defense” model, which clearly defines the roles and responsibilities of business units, compliance divisions, and internal audit services. The following table presents the general model of this system (Table 8.3).

Table 8.3 General model of the compliance risk management system

Line of defense	Level
First line of defense	Business units that accept and are responsible for compliance risk carry out ongoing compliance risk management
Second line of defense	Compliance department (division), which ensures the performance of compliance risk management functions and provides managers with confidence that the control and compliance risk management measures implemented by the first line of defense have been developed and are functioning properly
Third line of defense	Internal audit service, which verifies and evaluates the effectiveness of the compliance risk management system.

Source: Sheludko & Yegorova, 2017

Compliance risk management entities differ across sectors of the economy. In the manufacturing sector, the system is overseen by management, supported by a dedicated compliance risk management department, and implemented through the active involvement of employees. Internal audit departments, risk management divisions, and business units also play a crucial role in ensuring that compliance measures are properly integrated into operational processes.

In the financial services sector, responsibility lies primarily with the Supervisory Board and the Management Board. The compliance function is carried out by specialized departments and compliance officers, while internal audit departments and risk management divisions provide oversight and evaluation. Business units are directly engaged in applying compliance controls in their daily activities, ensuring that risks are managed effectively.

Within the education sector, compliance risk management is coordinated by the head and administration of the educational institution. The compliance officer and compliance department are responsible for implementing relevant policies and procedures. Staff members and students also contribute to maintaining compliance standards, thereby reinforcing the institution's reputation and ensuring adherence to ethical and regulatory requirements.

The effectiveness of compliance risk management is determined not only by organizational structures but also by the fundamental principles that guide their functioning. These principles ensure that compliance systems remain ethical, transparent, and adaptable to changing conditions. The following table outlines the key principles of compliance risk management and their main characteristics (Table 8.4).

Table 8.4 Principles of compliance risk management

Principle	Characteristic
Management Responsibility (“Tone at the Top”)	Management has strategic and ethical responsibility for implementing a compliance risk management system, creating policies, supporting a culture of integrity and responding to violations.
Risk-based approach	The compliance risk management system focuses on identifying, assessing, and prioritizing the risks that have the greatest impact on the organization – legal, reputational, and financial.
Compliance culture	It is formed through training, leadership example, open communication, and the encouragement of ethical behavior.
Independence	The compliance unit should be autonomous from operational structures to avoid conflicts of interest and ensure objectivity in controls and investigations.
Transparency	All processes, policies and decisions should be clearly documented, available for review, and violations should be transparently recorded and addressed.
Efficiency	The compliance risk management system should not be only formal, but effective: identify risks on time, prevent violations, and maintain business stability.
Constant monitoring	Regular monitoring of changes in legislation, employee behavior, and counterparty actions is the basis for the adaptability of the compliance risk management system.
Improvement	The compliance risk management system should be constantly updated, taking into account new risks, technologies, regulatory requirements and feedback.

8.3. Compliance risk management process

The compliance risk management process is typically structured as a sequence of interconnected stages, each of which ensures the systematic identification, assessment, and mitigation of risks. This step-by-step approach allows organizations to maintain stability, transparency, and adaptability in a dynamic regulatory environment.

Compliance risk management actions vary across different sectors of the economy. In the manufacturing sector, they include the implementation of a Code of Corporate Ethics and an Anti-Corruption Policy, as well as the promotion of a compliance culture through training, responsibility consolidation, and active involvement of management and

employees in key processes. Systematic monitoring of regulatory changes, identification and analysis of potential conflicts of interest, and the establishment of a hotline for reporting corruption offenses are also essential. Furthermore, procedures for verifying the business reputation and integrity of counterparties are introduced before establishing business relationships, with anti-corruption clauses incorporated into contracts.

In the financial services sector, compliance risk management focuses on organizing control over adherence to legislation and ensuring timely identification, measurement, monitoring, control, and reporting of risks. Continuous analysis of compliance risks is carried out, along with the evaluation of past events to prevent recurrence. Measures are taken to avoid decision-making that could expose the bank to significant risks, while compliance risks in relationships with clients and counterparties are closely monitored. Regular checks are conducted to ensure the absence of conflicts of interest, thereby strengthening institutional integrity.

Within the education sector, compliance risk management begins with defining a position or unit responsible for these functions and appointing a compliance officer who reports directly to the institution's leadership. Job descriptions and compliance programs are approved, and risk assessments are conducted within the institution. Transparency is ensured by publishing information about the progress of compliance risk assessments on the institution's website. Monitoring, reviewing, and evaluating the implementation of compliance measures are ongoing processes. Employees and students are actively involved through surveys that help identify vulnerable processes. Ethics and integrity committees are established to oversee compliance, while mechanisms for responding to violations and holding responsible individuals accountable are developed. Finally, compliance risk minimization is ensured across all institutional processes, including education, student assessment, admissions, dormitory accommodation, procurement, and the use of resources.

Different sectors of the economy apply diverse approaches to assessing compliance risks, reflecting their specific operational, regulatory, and cultural contexts. These approaches range from classical frameworks and quantitative-qualitative methods to risk-based strategies, gap analysis, instrumental techniques, and practical measures. The following table illustrates how these approaches are implemented in the manufacturing, financial services, and education sectors through concrete examples (Table 8.5).

Table 8.5 - Approaches to assessing compliance risks by sectors of the economy

Approach	Examples of implementation		
	Manufacturing sector	**Financial services sector**	**Education**
Classical	PJSC "Zaporizhzhia Metallurgical Plant "Zaporizhstal"" – risk management through ISO 31000:2018 and internal audits	JSC "Oschadbank" – implementation of internal regulations in accordance with the requirements of the NBU and FATF	KNEU named after V. Hetman – risk management cycle in the academic integrity system

Quantitative-qualitative	LLC “Nestle Ukraine” – analysis of risky operations based on rejection and complaint ratios	JSC CB “Privatbank” – client risk assessment by the number of transactions and type of business	Lviv Polytechnic National University – assessment of academic risk by number of violations and type of discipline
Risk-based	PJSC “ARCELORMITTAL KRYVYI RIH” – focus on critical occupational safety and environmental risks	JSC “Ukreximbank” – quarterly review of risks due to environmental changes	National University of Kyiv-Mohyla Academy”– adaptation of integrity policies to changes in the digital learning environment
GAP analysis	JSC “Kernel” – analysis of gaps between ESG practices and international standards	JSC “FUIB” – comparison of internal policies with AML/CFT requirements	Semen Kuznets Kharkiv National University of Economics – audit of compliance of educational programs with EQF standards
Instrumental	PrJSC “MHP” – “red flags” for identifying violations in supply chains	JSC “Ukrgasbank” , JSC “Raiffeisen Bank” – risk matrices, KRI, heat maps	Lviv Polytechnic National University – composite indicators for assessing the effectiveness of departments
Practical	JSC “Ukrenergomachines” – control over interaction with counterparties, periodic reporting	JSC “Kredobank” – monitoring changes in legislation, staff training	National Technical University “Kharkiv Polytechnic Institute” – training of teachers on ethics, reporting on conflicts of interest

Source: Chmutova, Bezrodna & Nechyporenko, 2020; Bortnikova, Stasyuk & Malynovska, 2020

In order to effectively identify, evaluate, and mitigate compliance risks, organizations across different sectors employ a variety of methodological tools. These methods provide structured approaches to risk assessment, ranging from visual techniques to quantitative indicators and early warning systems.

One of the most widely used methods is the risk matrix, which allows organizations to classify risks based on their probability and potential impact. In manufacturing, it is

applied to supply chains, particularly for assessing violations of environmental standards. Financial institutions use risk matrices to evaluate compliance processes, while in education they help identify risks related to academic integrity, such as plagiarism or conflicts of interest.

The risk heat map provides a visual representation of risks, highlighting their severity and likelihood. In the manufacturing sector, it is used to reflect occupational safety and environmental risks. Banks apply heat maps when launching new products to visualize potential compliance challenges, whereas universities use them in internal audits of educational programs to identify vulnerable areas.

Risk indicators serve as measurable signals of potential compliance issues. Manufacturing companies track indicators such as the frequency of quality standard violations or customer complaints. Financial institutions monitor complaints, policy violations, and delays in updating documents. In education, KRIs include the number of integrity violations and student complaints, helping institutions maintain ethical standards.

The «red flags» method is designed to detect early warning signs of misconduct. In manufacturing, it is used to identify conflicts of interest in procurement and tenders. Audit firms apply it to uncover fraud indicators such as unusually large payments or undue pressure on employees. In education, red flags highlight irregularities like unusual grades, pressure on teachers, or non-transparent procedures.

Finally, horizon scanning involves systematically reviewing and comparing compliance practices across different branches or units. Manufacturing companies use it to align ethics and security policies between branches. Banks apply it to compare anti-money laundering policies across offices, while universities use horizon scanning to evaluate integrity procedures across faculties, ensuring consistency and adaptability.

8.4. Tools and technologies

Internal mechanisms for controlling compliance risks play a crucial role in ensuring transparency, accountability, and ethical conduct across different sectors of the economy. These mechanisms include policies, training programs, monitoring tools, and third-party risk management practices, each adapted to the specific needs of manufacturing, financial services, and education. The following table outlines the main internal mechanisms applied in these sectors and highlights their content (Table 8.6).

Table 8.6. Internal mechanisms for controlling economic sectors

Mecha-nism	Content		
	Manufacturing sector	Financial services sector	Education
Politicies	Anti-corruption policy, Code of Ethics)	Anti-corruption policy, Code of Ethics; Bank Transparency and Accountability Policy	Anti-corruption policy, Code of Ethics, Code of Academic Integrity

Training	Annual training for staff on anti-corruption, ethics and conflict of interest prevention in the formats of online courses, interactive cases and testing.		
Monitoring	Automatic notification of risky transactions (e.g. unusually large payments, offshore transactions)	Monitoring is carried out through AML/KYC systems, specialized platforms for checking counterparties (LIGA360, YouControl), as well as IT solutions for transaction analysis	Plagiarism checking systems, Unicheck , StrikePlagiarism), trust boxes, pages on the website for reporting violations
Third-party risk management	Checking counterparties for sanctions, reputation, regular updating of the counterparty database, checking legal status, financial stability analysis, verification for conflicts of interest		

Technological solutions have become an integral part of compliance risk management, enabling organizations to automate processes, strengthen monitoring, and ensure transparency across different sectors of the economy. These tools range from ERP and CMS systems to AI-based anomaly detection and anti-plagiarism platforms, each tailored to the specific needs of manufacturing, financial services, and education. The following table presents the main technological solutions applied in these sectors and highlights their role in supporting compliance practices (Table 8.7).

Table 8.7 Technological solutions in compliance risk management by sectors of the economy

Manufacturing sector	Financial services sector	Education
In manufacturing, compliance covers anti-corruption measures, labor standards, and environmental responsibility. Technological solutions include ERP systems with compliance modules (e.g., SAP, Oracle, which integrate transaction and procurement control, and counterparty verification), CMS systems, platforms for counterparty verification (YouControl, Vkursi, Opendatabot , Clarity Project), AI for detecting violations	The financial sector has the highest level of regulatory control. Technological solutions focus on AML/KYC, sanctions monitoring, risk management, namely - KYC/AML automation includes OCR for reading documents, API for blacklist screening, ML for risk classification, generation of suspicious activity reports (SAR) - CMS systems (Banks integrate platforms that automatically check transactions for compliance with OFAC, EU, UN sanctions lists. Risky transactions are blocked or marked for manual verification. - AI for anomaly detection (Isolation Forest, XGBoost, LSTM)	In education, compliance focuses on academic integrity, ethical standards, and transparency in grant processes. Technology solutions include CMS platforms (Compliance Management System), anti-plagiarism systems (Unicheck, StrikePlagiarism), AI-based artificial text detectors, OCR, and API integrations.

8.5. Compliance Risks and the Path Toward Sustainable Governance

Compliance risks are a key factor determining the sustainability of organizations in the financial, manufacturing and education sectors. Their effective management makes it possible to minimize legal, reputational, and operational threats, ensuring trust from partners, regulators, and society.

Technological solutions – such as CMS systems, KYC/AML platforms, AI modules for monitoring – play a crucial role in detecting violations, automating control, and forming a systemic culture of responsibility. At the same time, it is the culture of integrity – the internal acceptance of ethical norms, openness to self-control, and willingness to act transparently – that is the foundation of sustainable compliance. In financial institutions, it is manifested through compliance with international standards, in manufacturing – through a responsible attitude towards employees and the environment, in education – through respect for intellectual property and transparency of scientific processes. In the context of European integration, Ukraine is gradually approaching EU standards, in particular through the harmonization of the regulatory framework, the development of digital platforms, the integration of artificial intelligence, and the strengthening of the role of independent compliance officers. This opens up prospects not only for technical modernization, but also for the formation of a new ethical governance paradigm based on transparency, trust, and sustainability.

Practical Exercises

Exercise 1 - Europeanization of ethical standards in teacher education using the example of the University of Vienna

The University of Vienna (Austria), within the framework of *the Europeanization in Teacher Education study*, faced the problem of fragmentation of ethical standards in teacher training and insufficient integration of European approaches to academic integrity. To tackle these challenges, digital platforms for monitoring the quality of education were introduced, ethical norms were harmonized and curricula were adapted to EU standards. As a result, the academic responsibility of teachers and students was increased, consistency of educational practices between European Union countries was ensured and a culture of integrity was strengthened as the basis for professional teacher training.

Task:

1. Read the case study about the University of Vienna's efforts to harmonize ethical standards and integrate European approaches to academic integrity in teacher training.
2. Answer the following questions:
   - > What challenges did the University of Vienna face in teacher education?
   - > Which measures were introduced to address these challenges?
   - > How did these measures contribute to strengthening a culture of integrity?
   - > In your opinion, why is academic integrity essential for professional teacher training?

3. Reflect on your own educational experience:

> Can you identify examples where academic integrity was emphasized or neglected?
> How could European standards improve teacher education in your country?

Format: Write a short essay (1–2 pages)

Exercise 2 - Compliance Control Automation in the FinTech Sector of Ukraine

Ukrainian fintech companies, including Monobank and Sportbank, faced current challenges in the field of financial security: money laundering risks, insufficient customer due diligence, and the threat of violating international sanctions regimes. To solve these problems, automated KYC/AML solutions were implemented, including integration with YouControl platforms, PEP databases, and sanction lists, as well as the use of artificial intelligence for behavioral risk assessment. As a result of these measures, the companies were able to significantly reduce the number of suspicious transactions, accelerate the onboarding process of new customers, and ensure compliance with the requirements of the National Bank of Ukraine and international FATF standards, strengthening trust in digital financial services.

Task:

1. Read the case study about Ukrainian FinTech companies (Monobank, Sportbank) and their implementation of automated compliance solutions.

2. Answer the following questions:

> What financial security challenges did Ukrainian FinTech companies face?
> Which automated solutions were introduced to address these challenges?
> How did these measures improve compliance and customer trust?
> Why is compliance with FATF standards and National Bank of Ukraine regulations crucial for FinTech development?

3. Reflect on broader implications:

> How can artificial intelligence enhance risk management in financial services?
> What risks might remain despite automation?

Format: Write a short essay (1–2 pages).

Exercise 3 - Non-compliance with anti-corruption policy in Ukrzaliznytsia

The state enterprise *Ukrzaliznytsia* has repeatedly been in the center of corruption scandals, in particular due to non-transparent tenders, conflicts of interest and ineffective control over procurement. The lack of a centralized CMS system, weak internal audit and a formal approach to anti-corruption policy led to a loss of trust from international partners, a decrease in investment attractiveness and the initiation of criminal proceedings against officials. This case demonstrates that without

technological support and ethical leadership, compliance remains declarative and is unable to prevent systemic violations.

Task:

1. Read the case study about Ukrzaliznytsia's repeated corruption scandals and weaknesses in compliance systems.

2. Answer the following questions:

> What were the main causes of corruption risks in Ukrzaliznytsia?
> How did the lack of technological support and weak internal audit contribute to systemic violations?
> What were the consequences of non-compliance for the enterprise and its international reputation?
> Why is ethical leadership essential for effective anti-corruption policy?

3. Reflect on broader lessons:

> How could digital compliance systems (CMS, audit tools) improve transparency in state enterprises?
> What role should international partners play in strengthening anti-corruption practices?

Format: Write a short essay (1–2 pages)

Target questions

1. What is compliance risk?
2. What does a risk management system include?
3. What factors can be sources of compliance risk?
4. What is the purpose of the compliance risk management system?
5. How many lines of defense does the overall compliance risk management model include?
6. Who are the subjects of compliance risk management?
7. What does the principle of "Tone at the Top" imply?
8. What approaches are used to assess compliance risks?

References for self-study

1. ISO 31000:2018 "Risk management". URL : dstu_iso_31000_2018.pdf
2. ISO 37301:2021 "Compliance management systems". URL: https://www.iso.org/obp/ui/en/#iso:std:iso:37301:ed-1:v1:en
3. Law of Ukraine "On Prevention of Corruption" dated 14.10.2014 № 1700-VII . URL: https://zakon.rada.gov.ua/laws/show/1700-18#Text
4. Law of Ukraine "On Public Procurement" dated 25.12. 2015 № 922-VIII. URL: https://zakon.rada.gov.ua/laws/show/922-19#Text

5. NBU Regulation “On the Organization of Risk Management Systems in Banks of Ukraine” dated 11.06.2018 № 64. URL: https://zakon.rada.gov.ua/laws/show/v0064500-18#Text
6. Law of Ukraine “On Capital Markets and Organized Commodity Markets” dated 23.02.2006 №3480-IV. URL: https://zakon.rada.gov.ua/laws/show/3480-15#Text
7. Law of Ukraine “On Education” dated 05.09.2017 № 2145-VIII. URL: https://zakon.rada.gov.ua/laws/show/2145-19#Text
8. Methodological recommendations on the application of tools and mechanisms for the transformation of various spheres of functioning of higher education institutions on the principles of transparency and integrity, approved by Order of the Ministry of Education and Science of Ukraine dated 17.04.2025 № 576. URL: https://mon.gov.ua/static-objects/mon/sites/1/news/2025/04/22/nakaz-576-vid-17-04-2025.pdf
9. Law of Ukraine “On Environmental Protection” dated 25.06.1991 № 1264-XII . URL: https://zakon.rada.gov.ua/laws/show/1264-12#Text
10. ISO 14001:2015 “Environmental management systems”. URL: https://surl.li/melazv
11. ISO 45001:2018 “Occupational health and safety”. URL : ISO 45001 2018 pdf free download - Industrial Engineering
12. Sheludko, S.A., & Yehorova, A.S. (2021). The essence of compliance and its place in banking risk management. *Modern Economics*, 26, 173-177. DOI: 10.31521/modecon.V26(2021)-26 [in Ukrainian]
13. Tkachuk, L., & Tkachuk, M. (2022). Peculiarities of educational institution management based on risk management. *Modern engineering and innovative technologies*, 22 (2), 80-87. DOI: 10.30890/2567-5273.2022-22-02-045 [in Ukrainian].
14. Bortnikova, M.H., Stasiuk, N.R., & Malynovska, Yu.B. (2023). Formation of applied compliance tools at domestic enterprises. *Menedzhment ta pidpryiemnytstvo v Ukraini: etapy stanovlennia ta problemy rozvytku*, 1 (9), 15-21. URL: menedzhment-15-21.pdf [in Ukrainian].
15. Anti-corruption compliance of higher education institutions: foreign experience and Ukrainian perspectives. (2023). *Analytical study*. Association of Legal Clinics of Ukraine, 60 p. [in Ukrainian].
16. Karpushenko, M., & Karpushenko, O. (2023). Theoretical and methodological aspects of forming a compliance control system. *Innovative technologies and scientific solutions for industries*, 1 (23), 132-142. DOI: 10.30837/ITSSI.2023.23.132 [in Ukrainian].
17. Chmutova, I.M., Bezrodna, O.S., & Nechyporenko, D.I. (2020). Methodological tools for assessing compliance risks of financial monitoring in banks. *Biznes-Inform*, 11 (2020), 296-309. URL: business-inform-2020-11_0-pages-296_309.pdf [in Ukrainian].

18. Risk matrix: A key tool in project risk management. (n.d.). *CASERS.* https://surl.li/hkargu [in Ukrainian].

19. Practical application of requirements for compliance risk management. (n.d.). *LIGA:ZAKON.* https://surl.li/ltgnos [in Ukrainian].

20. PwC Global Compliance Survey. (2025). *Time to act faster: How to reboot compliance to accelerate processes and overcome obstacles.* PwC Ukraine. https://www.pwc.com/ua/uk/survey/2025/komplaiens-2025.html [in Ukrainian].

21. Vodzianova, V. (n.d.). The role of the risk management unit in monitoring the effectiveness of the bank's internal control system. *Independent Association of the Banks of Ukraine.* https://surl.lu/hqiorm [in Ukrainian].

22. Tax compliance and basic elements of compliance risk management: the vision of the OECD and the IMF. (n.d.). *Visnyk. Ofitsiino pro podatky.* https://surl.li/mzglwu [in Ukrainian].

Assignments for Self-Study

1. Identify the main compliance risks in the financial, manufacturing, and education sectors. Compare them with operational and strategic risks. Prepare a short essay (1–2 pages) explaining why compliance risks are often more reputationally dangerous than financial or operational risks.
2. Describe the role of each line of defense in your own words. Choose one sector (manufacturing, finance, or education) and illustrate how the model works in practice. Suggest one improvement to strengthen the independence of the second line of defense.
3. Using Table 8.4, select two principles (e.g., Transparency and Risk-based approach). Provide real-life examples of how these principles could be applied in a university setting. Reflect: Which principle is hardest to implement in practice, and why?
4. Compare the quantitative-qualitative approach in finance (Privatbank) with the instrumental approach in education (Lviv Polytechnic). Design a mini risk matrix for your chosen institution (manufacturing company, bank, or university). Highlight at least three «red flags» relevant to that institution.
5. Choose one technological solution (ERP, AML/KYC automation, or anti-plagiarism systems). Explain how it helps prevent compliance risks. Discuss possible limitations of relying too much on technology in compliance risk management.
6. Write a short reflection (1 page) on how compliance culture contributes to sustainable governance. Compare the role of integrity in financial institutions vs. universities. Suggest one innovative way to strengthen compliance culture in your own environment.

Chapter 9: Anti-Corruption Policy and Corporate Compliance

Learning outcomes

After studying this section, students will be able to:

- Know and understand the concept and content of anti-corruption policy, its main elements, as well as the role and significance of the latter for the compliance management of the enterprise.
- Know the key corruption risks and methods and means of their detection, assessment, and elimination/minimization.
- Know the main and auxiliary subjects of preventing and combating corruption and differentiate their powers depending on the level and scope of activity.
- Analyze the effectiveness of anti-corruption compliance programs, taking into account national anti-corruption legislation and local monitoring and control tools.
- Identify and develop effective measures to increase transparency, integrity, and corporate responsibility.

Key words: anti-corruption policy, corporate compliance, corruption risks, integrity, management, whistleblower, compliance program, undue advantage, conflict of interest.

Key definitions

Corruption – the use by a person of powers related to their official activities for the purpose of obtaining or accepting a promise/offer of unlawful benefit for themselves or a third party (parties) in order to induce such a person to misuse their official powers.

Anti-corruption policy – a set of organizational and legal measures to prevent corruption, which form (ensure) the content and procedure for applying preventive anti-corruption mechanisms, as well as auditing and monitoring the results of their application.

Corruption risk – conditions and causes that contribute to or cause/facilitate the commission of a corruption or corruption-related offense by a public official.

Unlawful benefit – tangible or intangible assets that are promised/provided or received without legal grounds for the performance or non-performance of official duties by a person.

Conflict of interest – potential or actual conflicts between an individual's personal and professional interests that may create corruption risks and/or threats.

Integrity – a set of professional and moral-ethical values and norms that determine the rules of conduct in the performance of official duties.

Corporate compliance – a set of organizational and legal measures aimed at ensuring

that the internal policies of an enterprise comply with national regulations, international and European standards, and ethical norms in professional activities.

Internal control – a set of managerial and organizational and legal measures aimed at ensuring the timely identification of risks and threats that may arise in professional activities.

Standards, legislative and other regulatory acts

1. International standards: ISO 37001:2016 - Anti-bribery Management Systems (ABMS); ISO 37301:2021 - Compliance Management Systems; ISO 37002:2021 - Whistleblowing Management Systems; ISO 31000 - Risk Management - Guidelines; ISO 37000 - Governance of Organizations - ISO 37000 - Governance of Organizations;

2. European Union (EU): Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law; Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC; Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC; Directive 2014/23/EU of the European Parliament and of the Council of 26 February 2014 on the award of concession contracts; Directive (EU) 2017/1371 of the European Parliament and of the Council of July 5, 2017, on the fight against fraud affecting the financial interests of the Union by means of criminal law; Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (Market Abuse Regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC; Directive (EU) 2022/2464 of the European Parliament and of the Council of December 14, 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting;

3. International law: Criminal Law Convention on Corruption (ETS 173); United Nations Convention against Corruption; Civil Law Convention on Corruption; Convention on Combating Bribery of Foreign Public Officials;

4. American law: American and English Acts: Foreign Corrupt Practices Act; UK Bribery Act;

5. Ukraine: Law of Ukraine No. 1700-VII dated October 14, 2014, «On Preventing Corruption»; Law of Ukraine No. 2322-IX of 20 June 2022 «On the Principles of State Anti-Corruption Policy for 2021-2025»; documents of the National Agency for Corruption Prevention; codified acts regarding legal liability for corrupt practices.

List of Subchapters

9.1 The organizational, legal, and ethical role of anti-corruption policy

9.2 Institutionalization of integrity in corporate governance and the role of the manager

9.3 Corruption risks in corporate governance and their neutralization through internal control

9.4 Current issues and prospects for the development of corporate compliance

9.1 The Organizational, Legal, and Ethical Role of Anti-corruption Policy

Anti-corruption policy is a comprehensive concept that forms the basis for the formation and development of the institution of integrity. The content of anti-corruption policy is determined by a set of standards and provisions of legislative and other regulatory acts based on international and European recommendations and requirements, which regulate the activities of the state in the field of preventing and combating corruption. Accordingly, anti-corruption policy is differentiated into several levels:

1. National anti-corruption policy – as a rule, it is an anti-corruption strategy for a specific period of time, as well as a state anti-corruption program.

For example, in Ukraine, Resolution No. 220 of the Cabinet of Ministers of Ukraine dated March 4, 2023, approved the State Anti-Corruption Program for 2023-2025, which aims to achieve significant progress in preventing and combating corruption, ensuring the coordination and consistency of anti-corruption activities of all state and local government bodies, as well as the proper process of post-war reconstruction of Ukraine (State Anti-Corruption Program for 2023-2025, approved by Resolution of the Cabinet of Ministers of Ukraine No. 220 of March 4, 2023); and Law of Ukraine No. 2322-IX of June 20, 2022, «On the Principles of State Anti-Corruption Policy for 2021-2025,» approved the Anti-Corruption Strategy for 2021-2025, which aims to achieve significant progress in preventing and combating corruption, as well as ensuring the coordination and consistency of anti-corruption activities of all state authorities and local self-government bodies. This Anti-Corruption Strategy considers corruption to be a key obstacle to stable economic growth and the development of effective and inclusive democratic institutions (Anti-Corruption Strategy for 2021-2025, approved by Law of Ukraine No. 2322-IX of June 20, 2022, «On the Principles of State Anti-Corruption Policy for 2021-2025»);

2. Local anti-corruption policy – formed taking into account national principles of preventing and combating corruption and, as a rule, reproduced in an anti-corruption program adopted by local self-government bodies and implemented within a specific territorial unit (region/oblast, etc.);

3. Local anti-corruption policy – a set of internal legal documents and programs aimed at eliminating corruption risks of a specific business entity.

The proper quality of an entity's anti-corruption policy makes it possible to form an ethical corporate culture, since it is through principles that are defined and acceptable in the local business environment that the principles of internal hierarchy, as well as rules of conduct and interaction between entities, their business partners, and stakeholders, are determined.

A study conducted by the Organization for Economic Cooperation and Development

found that the landscape of anti-corruption efforts has changed in recent years; once led by governments and their law enforcement agencies, the private sector has become an increasingly important player. Companies around the world have invested in developing anti-corruption compliance programs and recognize that these investments should, in essence, prevent corruption. The importance of evaluating the effectiveness of compliance programs has long been emphasized by international standards. As companies take steps to develop anti-corruption compliance programs, they must also take steps to evaluate these programs to ensure their effectiveness in preventing corruption. In practice, companies' evaluation efforts are driven by at least three factors. Chief among these is the avoidance of sanctions or reputational damage, a reactive approach motivated by risk-related issues.

Companies also conduct assessments to provide evidence that anti-corruption measures contribute to business success, which helps compliance staff legitimize and secure investment in compliance. Finally, assessments can promote a proactive approach to compliance that involves holistically promoting a corporate culture of integrity. While commendable, moving away from a reactive, rules-based approach requires companies to focus more on long-term compliance goals and corporate values, as well as to engage the appropriate skills and resources. Performance evaluation requires companies to first define what constitutes an effective anti-corruption program and then evaluate the program based on desired outcomes. This means that compliance staff identify goals (e.g., risk reduction) and initiatives that can be taken to achieve them. A risk-based approach is central to companies' assessment efforts, but it can be complemented by a proactive approach that promotes ethical corporate behavior. This enhances the effectiveness of compliance programs by fostering a sense of responsibility among staff. Measuring and evaluating effectiveness also requires companies to collect data so they can take appropriate action to improve their programs. Evidence-based measures that support evaluation include conducting root cause analysis, transactional testing, and testing anti-corruption training programs. Engaging senior and middle management in promoting and implementing anti-corruption standards is fundamental to the effectiveness of anti-corruption programs and should be a key element in assessments. Mobilizing multidisciplinary teams to ensure proper implementation of compliance efforts across all corporate functions also supports a comprehensive assessment of anti-corruption programs, reflecting companies' recognition that cultivating an ethical corporate culture is a shared responsibility. (Companies' assessments of anti-corruption compliance, OECD 2025).

Practical case study. *In 2013, the well-known British company Rolls-Royce was accused of implementing multiple corruption schemes aimed at winning tenders. The British newspaper The Guardian reported that the Serious Fraud Office (SFO) had launched a formal criminal investigation into allegations of bribery and corruption at Rolls-Royce. The aerospace and defense company has been in the spotlight since late 2012, when it announced that the SFO had approached it regarding allegations of wrongdoing in Indonesia and China, prompting Rolls-Royce to conduct an independent investigation that revealed «matters of concern.» Rolls-Royce hired law firm Debevoise & Plimpton to investigate allegations of corruption made public by a former employee who had worked at Rolls for over 30 years, particularly in Indonesia, and became a whistleblower after the company ignored concerns he raised internally that the*

company had a «secret fund to cover up information.» The investigation revealed concerns about the company's activities in China, which were referred to the SFO. To demonstrate its seriousness about the allegations, Rolls-Royce appointed Lord Gold, a former City lawyer and Conservative Party colleague, in January to review its anti-bribery and compliance procedures. It was reported that the company tried to avoid a formal SFO investigation by offering to pay a multi-million pound fine (The Guardian: Rolls-Royce: SFO launches formal bribery and corruption investigation). As a result, Rolls-Royce issued an «unreserved apology» after agreeing to pay more than £600 million to settle a long-running corruption case (Parsons, A., 2017).

This case study highlights several important compliance insights:

1. The company lacked an ethical corporate culture, which made it impossible to independently identify corruption and the risks of its intensification in a timely manner, as confirmed by the testimony of their former employee regarding the disregard of his attempts to resolve the issue by initiating an internal corporate investigation.

2. Despite being a large international corporation, Rolls-Royce did not have a systematic approach to the formation and implementation of an anti-corruption policy, which resulted in significant reputational and material losses.

3. In fact, only these losses necessitated a review of the anti-corruption compliance security system.

Thus, anti-corruption policy is a legal collective concept, as it is formed from a symbiosis of legislative provisions and ethical standards and is based on specific international and European anti-corruption standards. At the same time, the concept of anti-corruption policy is always closely interrelated and interdependent with the concept of integrity policy.

9.2 Institutionalization of integrity in corporate governance and the role of the manager

Integrity is a key management resource that shapes the investment attractiveness of a business entity. Since integrity is a management resource, the quality of integrity policy/culture, and therefore the implementation of anti-corruption policy and corporate compliance measures, depends primarily on the ability of the manager not only to establish, but also to comply with and ensure compliance with established corporate requirements by others.

Organizational integrity is a company's inherent ability to adhere to the principles of self-sufficiency in the sense that its activities are based on an internally consistent system of principles and reflect the extent to which applicable legal norms and standards are implemented in the organization's actions. A certain maturity is required in terms of the company's infrastructure and its CID [corporate internal decision-making] structures. Organizational integrity includes the ability to self-assess and recognize both the strengths and weaknesses of the organization, leading to the ability to mature further (in the sense of further development). Finally, organizational integrity requires

desirable moral principles such as compliance with legal requirements, honesty, and respect (Fuerst, Luetge, 2021, p. 6; Fuerst, Madeleine J.; Luetge, Christoph; Max, Raphael; Kriebitz, Alexander, 2023). Operationalized organizational integrity means that a company: 1) actively commits to adhering to self-imposed norms and principles; 2) transparently institutionalizes these commitments in its CID structures; and 3) ensures that these commitments are implemented in action. (Madeleine J. Fuerst | Christoph Luetge, 2021).

Institutionalizing integrity involves creating internal policies and standards of conduct within the company, developing compliance systems and codes of ethics, and ensuring that these tools can be used in all corporate procedures. Corporate/organizational integrity ensures the transparency of a business entity's activities—from personnel policy to the quality and consequences of certain management decisions. The quality of the relevant measures depends on management policy and the role of the manager responsible for shaping the organizational culture. It is the manager, who is an ethical leader, who guarantees the transparency and accountability of the enterprise's activities.

Ethical leadership involves setting and achieving ethical goals and influencing others in an ethical manner. Contemporary approaches to ethical leadership focus on the interpersonal component of leadership by analyzing how ethical leaders exercise power and influence. In summary, it is clear that individuals in power must synchronize ethics with the pragmatism required by leadership in order for employees to perceive them as ethical leaders. Otherwise, they are likely to be seen as hypocrites if they do not practice what they preach, as hypocritical leaders talk about the importance of ethics, but their actions show that they can be dishonest and unprincipled (Ferhani, B., 2025).

Corporate culture is a fundamental aspect that determines the success and development of any organization. It brings together shared values, beliefs, and behavioral norms, creating a special atmosphere that influences all aspects of the company's activities. Leadership plays a special role in shaping and maintaining corporate culture, as it is the leaders who determine which values and standards will be prioritized. Different leadership styles - from autocratic to democratic and liberal - have different effects on corporate culture, and their choice should be motivated by the needs of the organization and its strategic goals. Successfully forming and maintaining a productive corporate culture requires leaders to possess a set of key qualities covering personal, professional, social, value-based, and marketing aspects. These qualities not only promote team cohesion and increase work efficiency, but also create a stable environment conducive to innovation and development. Corporate culture is a fundamental element that influences all aspects of organizational life, with people at the center of this culture and their mutual respect and personal development being the key to creating a positive and productive work environment. Leaders play a crucial role in shaping and maintaining corporate culture by implementing it through a system of primary and secondary mechanisms that demonstrate core values and standards of behavior (Khrapkin, V., Khrapkin, O., 2024).

The potential results and consequences of a business entity's activities, its investment attractiveness, as well as possible image losses that may arise due to untimely detection and/or ignoring of corruption risks and threats depend on the managerial

activities of the leader. A breach of integrity at any stage of management activities or inadequate monitoring of administrative, operational, or strategic processes during the implementation of any corporate procedure may lead to a violation of anti-corruption rules and corresponding materially unsatisfactory consequences.

Practical case study: *In November 2006, regulatory investigations into German engineering giant Siemens revealed that hundreds of employees had spent millions of euros on «fake consulting contracts, false invoices, and shell companies» to pay huge bribes to secure contracts. The trial judge described it as «a system of organized irresponsibility that was implicitly approved» (senior management used removable stickers to authorize potentially compromising documents). This scandal embarrassed Siemens not only in the eyes of angry shareholders and investors, but also in the eyes of the German public, and humiliated its employees. Its reliability came under scrutiny, its integrity was questioned, as was the benevolence of its senior management, which seemed to have tolerated such practices. One of the leading shareholder groups questioned the basic competence of the Board of Directors in handling the case. However, Siemens' overall response to the scandal was widely praised by many independent experts on anti-corruption and ethics, including the Organization for Economic Cooperation and Development and the US federal government.*

At the outset, Siemens appointed Michael Hershman, co-founder of Transparency International, as its advisor - a shrewd move aimed at collaborating with a leading anti-corruption expert. Siemens implemented new, strict anti-corruption/compliance rules and procedures. It hired more than 500 full-time compliance staff (up from 86 in 2006) and a former Interpol employee to head a new investigative unit. It also created compliance hotlines and an external ombudsman position that operates worldwide and online. The company created a web portal for employees to assess risks in their interactions with customers and suppliers. In an effort to change its internal culture, Siemens launched a comprehensive anti-corruption training and education program for its employees. By 2008, Siemens had trained more than half of its 400,000 employees worldwide on anti-corruption issues. Siemens announced that it would avoid competition in certain known hotbeds of corruption or unethical practices, such as Sudan - a simple gesture, albeit one that does not significantly punish the company financially.

More significant was the decision to voluntarily suspend applications for World Bank financing for two years. A 15-year program to pay $100 million to non-profit organizations fighting corruption was also agreed upon. Ultimately, the firm took more than 900 internal disciplinary measures, including dismissals. In addition to the staff amnesty, Lesher replaced Siemens' extremely complex matrix structure with a simpler one consisting of only three divisions, whose directors sit on the board of directors. Millions of bank statements, documents, and transactions were reviewed. In total, the scandal cost Siemens €2.5 billion, including €2 billion in fines. The company was also banned from working with certain customers. It is difficult to calculate the cost of two years of public scrutiny for employees, especially in Germany. Lescher, who is still CEO of Siemens, was praised for his approach to fighting corruption, but he argued that changing the corporate culture to one guided by ethical standards «is a marathon for us, not a sprint.» However, by June 2008, some executives were confident enough to declare Siemens «the cleanest company.» (Dietz, G., Gillespie, N. (2012); The Guardian: Rebuilding trust: How Siemens atoned for its sins, 2012).

This case study highlights several important compliance insights:

1. Systemic tolerance of corrupt practices determines the scale of their consequences. If a corporation's ethics allow or tolerate breaches of integrity, compliance mechanisms will not work.

2. For a corporation, reputational losses are always more serious than material losses. Corporate ethics and integrity are resources for increasing efficiency and financial capacity, and therefore reputational risks must be taken into account when developing compliance security measures.

3. Ethical culture is the result of the systematic activities of a leader who shapes values and behavioral standards. Ensuring proper compliance security and integrity should be a corporate rule that must be followed first and foremost by the manager. Only by creating conditions in which ethical behavior is the exclusive form of behavior can the strategic value of corporate ethics be formed, and the manager become the guarantor of transparency in management activities.

9.3 Corruption risks in corporate governance and their neutralization through internal control

The low effectiveness of internal anti-corruption controls is the main reason for identifying corruption risks and threats, especially in companies and organizations with complex structures and poor corporate ethics. The above examples of corruption incidents that have occurred at global companies confirm the importance of compliance procedures that must be implemented at the local level.

The main corporate corruption risks can be divided into several large groups:

1. Corruption risks arising in the management system at the highest level. This group of corruption risks, associated with the unsatisfactory functioning of top management, has the most destructive impact. Conflict of interest is a determining factor, a key sign of corruption, and a prerequisite for promoting one's own interests. In particular, this applies to cases where a manager begins to use information asymmetry to obtain unlawful material benefits.

Scientists determine that it is expedient to define agency relations as an agreement under which one or more persons (principal(s)) engage another person (agent) to perform a specific service on their behalf, which involves delegating certain decision-making powers to the agent. If both parties to the relationship are utility maximizers, there are good reasons to believe that the agent will not always act in the principal's best interests. The principal can limit deviations from their interests by setting appropriate incentives for the agent and incurring monitoring costs aimed at limiting the agent's anomalous behavior. In addition, in some situations, it will be beneficial for the agent to spend resources (bond costs) to ensure that he does not take certain actions that would harm the principal, or to ensure compensation for the principal if he does take such actions. However, as a rule, it is impossible for the principal or agent to guarantee at zero cost that the agent will make optimal decisions from the principal's point of view. In most agency relationships, the principal and agent incur positive costs for

monitoring and providing guarantees (both intangible and monetary), and in addition, there will be some discrepancy between the agent's decisions and those decisions that maximize the principal's welfare. The dollar equivalent of the reduction in welfare that the principal experiences due to this discrepancy is also the cost of the agency relationship, and we call this latter cost «residual losses.» (Jensen Michael C., Meckling William H., 1976).

In fact, corruption risks in the sphere of top management activities make it impossible to develop and implement adequate anti-corruption policies. A manager who is interested in violating the principles of integrity similarly influences subordinates, which leads to tolerance of corruption, conflicts of interest, and negative attitudes toward initiatives aimed at strengthening internal control. Regarding the latter point, the above example of the Rolls-Royce corruption scandal is a striking illustration.

2. Corruption risks arising at the operational management level. At this level, corrupt acts are committed more frequently, since it is at this stage that the direct activities of the business entity are carried out. Most transactions carried out at this stage have a prolonged effect or are multi-act or systemic, which complicates and sometimes makes it impossible to detect corruption risks or corruption offences in a timely manner.

3. Corruption risks arising from interactions with external partners. This set of risks is directly related to the fact that global corporations, enterprises, and companies, as well as a number of other business entities with high investment attractiveness, cooperate with foreign and international partners, which, if the principle of integrity is violated, can lead to transnational corruption. Such risks usually require the development of compliance control measures, differentiated in accordance with the corporate culture and legislation of the state in which the business entity operates and the partner state.

4. Corruption risks associated with an unsatisfactory level of corporate ethics and culture. As mentioned above, the lack of integrity makes it impossible to create an effective anti-corruption policy. The normalization of corruption offenses, reduced sensitivity to violations of cultural and ethical norms, tolerance of non-tax income, an inflexible remuneration system, and unsatisfactory leadership on the part of managers create a system of corruption risks and destroy corporate ethical barriers.

The role of internal control in overcoming corruption risks is to create an effective mechanism for their prevention and/or detection. The following tools can be used to prevent corruption risks:

1) development and implementation of an internal anti-corruption strategy, code of ethics, and specific measures to implement the tasks assigned to the business entity;

2) clear differentiation of the powers and functional duties of employees, the limits of their vertical and horizontal subordination, timely detection and elimination of conflicts of interest;

3) creation of transparent automated and integrated digital systems/programs, etc., aimed at ensuring timely access to all information of the business entity by the manager and persons performing internal audit.

The creation of an electronic document management system, as a rule, reduces the risk of covert corrupt activities by employees by 40-50%. Similarly, the above methods also ensure the detection of corruption risks.

Practical case study: *In 2010, the automotive concern Daimler AG was accused of large-scale bribery involving multiple incidents. «In a decade-long scheme involving tens of millions of dollars, Daimler AG and three of its subsidiaries brazenly offered bribes in exchange for business around the world.» «Using offshore bank accounts, third-party agents, and deceptive pricing practices, these companies viewed bribing foreign officials as a way of doing business. The plea agreements and deferred prosecution agreements entered into today by Daimler AG and its subsidiaries should serve as a signal to other companies subject to the FCPA that do business around the world that corrupt business is bad business.» In connection with its admission of guilt, DCAR acknowledged that it made improper payments to Russian federal and municipal government officials to secure contracts for the sale of vehicles by inflating customer invoices and returning the excess amount to government officials or other designated third parties who did not provide any legitimate services to DCAR or Daimler AG. At the request of DCAR or Daimler AG employees, bank transfers were made from Daimler AG bank accounts in Germany, among other destinations, to bank accounts in the United States and Latvia belonging to fictitious companies, with the understanding that the money was, in whole or in part, intended for the benefit of russian government officials. In connection with its guilty plea, ETF admitted that it made corrupt payments directly to Croatian government officials and third parties, including two US-based corporate entities, with the understanding that the payments would be passed on, in whole or in part, to Croatian government officials to facilitate the sale of 210 fire trucks. In connection with the deferred prosecution agreement, DCCL admitted that it made improper payments in the form of commissions, delegation trips, and gifts to Chinese government officials or their designees in connection with the sale of commercial vehicles and Unimog vehicles to various Chinese government customers. DCCL acknowledged that in some cases it used US-based agents to facilitate the payment of bribes. Under the terms of the deferred prosecution agreement, Daimler AG agreed to hire an independent compliance monitor for three years to oversee the company's ongoing implementation and maintenance of its FCPA compliance program, as well as to report to the company and the Department of Justice. DCAR, ETF, and DCCL are subject to the monitoring provisions of the deferred prosecution agreement with their parent company, Daimler AG. Daimler AG has also agreed to cooperate fully with U.S. and foreign authorities in investigations of the company's corrupt payments. Today, Judge Leon also issued a separate ruling against Daimler AG, resolving a related civil complaint filed by the U.S. Securities and Exchange Commission (SEC). Daimler AG agreed to pay $91.4 million in disgorgement of profits related to these violations (Office of Public Affairs, 2010*).

This case study highlights several important compliance insights:

1. The existence of a formalized compliance culture makes it impossible to create an adequate and effective anti-corruption policy, and therefore, in such cases, alternative management systems, conflicts of interest, etc. always arise.

2. If a company has subsidiaries, the anti-corruption and integrity measures of each of them must comply with the corporate ethics of the head office. Ignoring the importance of creating a centralized model for controlling the activities of subsidiaries always increases the risk of their increased vulnerability to corruption.

3. Information asymmetry in top management leads to distortion in the management system, which creates conflicts of interest.

Accordingly, the effectiveness of internal control in overcoming corruption risks lies in increasing investment attractiveness, reducing image and material risks, strengthening the corporate culture of integrity, etc.

9.4 Current issues and prospects for the development of corporate compliance

The modern business environment is a dynamic phenomenon that is constantly evolving and becoming more complex. Under such conditions, the role of compliance becomes increasingly important, as the globalization transformations taking place in the state and society require a timely response to a number of unsatisfactory corruption processes that negatively affect not only the internal system of economic entities, but also the economic system and security of the state as a whole.

In the context of active development of the state and society, the main compliance challenges are as follows:

1. Dynamism of legislation. Currently, European countries are actively developing, in particular, creating new state and legal institutions, expanding the list of possible administrative services, and developing external relations with other partner countries. Accordingly, any active development requires updating regulatory legislation, the purpose of which is to ensure the proper functioning of such institutions. Updating state legislation is always accompanied by the need to adapt companies' internal legal documentation to it. In this regard, there is a need for constant monitoring and stabilization of the activities of business entities in line with legislative changes. Untimely or incorrect resolution of such a problem can not only lead to material and image losses, but also contribute to the formation of new corruption risks.

2. A formal approach to corporate ethics and integrity. Staff working in the business sector should view compliance as a system of tools capable of strengthening internal anti-corruption policies. A formal approach to an entity's anti-corruption policy reduces the effectiveness of relevant compliance procedures and negatively affects corporate integrity and the transparency of corporate procedures. Accordingly, this also applies to corporate ethics.

The anti-corruption compliance policy is a systematic document that formulates the basic principles, objectives, and responsibilities aimed at preventing, detecting, and responding to corruption risks in the organization's activities. This policy is the basis for the implementation of anti-corruption measures and defines the ethical standards of conduct that all employees must adhere to, regardless of their job responsibilities. The anti-corruption compliance policy covers key aspects such as the prohibition of bribery, corruption schemes, and resource manipulation, and defines the rules for interacting with partners, contractors, and other external stakeholders. It establishes clear criteria for identifying corruption risks and mechanisms for monitoring them, including procedures for reporting violations and anonymous reporting channels. In addition, it should be noted that the anti-corruption compliance policy should include

provisions for training and raising employee awareness of anti-corruption standards, as well as establishing responsibility for compliance with these standards. This provides not only a legal but also an ethical basis for anti-corruption activities, fostering an understanding among employees of the importance of preventing corruption as part of corporate culture (Lyubimov, V., 2025).

Corporate culture acts as a tool for coordinating activities, ensuring that employees work together to achieve strategic goals. Its integration at all levels of management allows for the formation of a shared vision and value orientation, which reduces internal conflicts and contributes to increased productivity. In addition, corporate culture is the basis for motivating staff, strengthening their loyalty and engagement, which is especially important in a competitive business environment. Corporate culture, therefore, is not only a reflection of the values and principles of the organization, but also an active factor in its development. Its influence covers all aspects of organizational activity — from strategic planning to the management of daily processes. Effective corporate culture management allows organizations to adapt to external challenges, ensure harmonious development of the internal environment, and improve the overall efficiency of the organization. Business ethics is an integral part of modern management, defining the moral basis for decision-making and regulating interactions between all participants in business processes. In the context of management processes, it plays the role not only of an element of corporate culture, but also of an effective tool for strategic development, ensuring a balance between the economic goals of the organization and social responsibility. It forms the basis for responsible decisions that meet not only the internal interests of the organization but also public expectations, reducing reputational risks and strengthening stakeholder trust (Perepelytsia, S., 2025).

3. Intensification of cyber threats. In the context of active informatization and digitization of business activities and administrative services, the issue of increasing cyber threats is becoming increasingly relevant. The implementation of most corporate procedures through the use of various online platforms, such as electronic public procurement systems (in Ukraine – Prozorro), has a qualitative impact on the implementation of compliance procedures, but at the same time, the loss of relevant data may result in the unlawful disclosure of personal data or data related to official activities, leading to civil, and sometimes administrative or criminal liability for those responsible. Accordingly, strengthening the mechanism for protecting corporate compliance from cyber threats is currently one of the priority tasks that need to be addressed.

Current challenges shape future trends in corporate compliance and global and local anti-corruption policies. These trends include:

1) strengthening the mechanism for ensuring the activities of whistleblowers. Currently, it is important to define an algorithm for protecting whistleblowers by increasing the institutional capacity of relevant entities to prevent and combat corruption, as well as improving the quality of the regulatory and legal framework for such activities. Another relevant area is simplifying the procedure for whistleblowers to report corruption;

2) improving the quality of the implementation of international and European standards in national legislation on the formation of anti-corruption and corporate legislation in order to coordinate international activities in this area;

3) Integration of artificial intelligence into compliance procedures. The use of artificial intelligence in corporate compliance will make it possible to respond more quickly to key corruption risks and threats, as well as to develop more tailored and balanced sets of appropriate anti-corruption measures. Another positive aspect should be the establishment of interaction between humans and artificial intelligence, which will make it possible to reduce the incidence of negative human factors, while at the same time allowing for critical assessment of compliance procedures by relevant specialists;

4) inclusion of compliance in strategic management. The inclusion of compliance in strategic management is an almost obvious consequence of the development of the state and society. The formation of a unified concept of strategic management, the diversification of entities involved in preventing and combating corruption, and the differentiation of their powers in accordance with external and internal procedures indicate the advisability of considering compliance an integral part of strategic management.

Practical Exercises

Exercise 1 – Establishing elements of anti-corruption policy

Script:

The Ukrainian company plans to update its internal anti-corruption policy in accordance with international/European standards and the Law of Ukraine «On Prevention of Corruption.»

Tasks:

> Identify the key elements of internal anti-corruption policy (taking into account ISO 37001, ISO 37301, ISO 31000).

> Explain the role of integrity in corporate culture.

> Explain why the absence of a clear anti-corruption policy leads to reputational and operational risks.

Exercise 2 – Classification of corruption risks

Script:

The company conducts audits and monitors corruption risks.

Tasks:

> Classify corruption risks (top management, operational level, external partners, corporate ethics).

> Give an example of a possible risk for each group.

> Suggest internal control tools that can minimize each type of risk.

Exercise 3 – Negative consequences of ignoring internal messages

Script:

An employee reported a possible violation of integrity rules and requirements to management, but the information was ignored (Rolls-Royce case).

Tasks:

> Explain what systemic compliance failures led to the corruption scandal at Rolls-Royce.

> Identify three lessons for Ukrainian companies.

> Propose mechanisms to prevent internal reports from being ignored.

Exercise 4 – The role of leaders in institutionalizing integrity

Script:

The company has a new director, and we need to assess how this will affect corporate culture.

Tasks:

> Describe why ethical leadership determines the level of integrity of an organization.

> Give examples of management decisions that positively and negatively affect compliance culture.

> Explain what «organizational integrity» means.

Exercise 5 – Analysis of corruption risks in subsidiary structures

Script:

The international corporation has several subsidiaries operating in Ukraine.

Tasks:

> Based on the Daimler AG case study, determine why subsidiaries often become the «weak link» in a compliance system.

> Explain the importance of centralized control and standardization.

> Develop three preventive measures for subsidiaries.

Exercise 6 – Developing a code of ethics

Tasks:

> Propose a structure for the company's code of ethics (values, conflicts of interest, interaction with stakeholders, mechanisms for reporting violations).

> Explain the role of corporate culture in shaping ethical standards.

> Provide examples of provisions that strengthen staff integrity.

Exercise 7 – Assessment of internal controls and identification of weaknesses

Script:

An audit of compliance measures was conducted, which revealed significant gaps in the accounting and management of business activities.

Tasks:

> Explain why internal control is key to overcoming corruption risks.

> Provide examples of weaknesses in corporate processes that may contribute to corruption.

> Propose an approach to eliminate them (digitalization, automation, auditing, role of compliance officer).

Exercise 8 – The impact of corporate ethics on corruption risks

Script:

The company is showing signs of declining corporate ethics: employees tolerate minor violations, and indifference to integrity policies is emerging.

Tasks:

> Analyze why a decline in sensitivity to ethical standards increases the number of corruption risks.

> Explain, based on the material, how leadership influences the «normalization of deviations.»

> Propose a set of measures to restore corporate integrity.

Exercise 9 – Current challenges of corporate compliance

Script:

The company is transitioning to digital systems and integrating new technologies, but is concerned about cyber threats and information leaks.

Tasks:

> Explain the main contemporary challenges of corporate compliance (changes in legislation, formalism, cyber risks).

> Analyze why the use of AI can be both an opportunity and a risk.

> Propose solutions to improve the cyber resilience of anti-corruption procedures.

Target Questions

1. What role does anti-corruption policy play in shaping an organization's integrity system?
2. How do national and international anti-corruption regulations combine in shaping compliance requirements for businesses?
3. Why is it important to regularly assess the effectiveness of a compliance program, and what indicators can demonstrate its quality?
4. How does organizational integrity differ from individual integrity, and why is it considered a strategic resource for a company?
5. What mechanisms contribute to the institutionalization of integrity in the corporate governance system?
6. How do ethical values influence employee behavior, decision-making, and the long-term reputation of an organization?
7. What is ethical leadership and why is it a key factor in shaping corporate culture and anti-corruption resilience?
8. How can management behavior both strengthen and undermine a system of corporate integrity and compliance?
9. What management practices demonstrate a commitment to transparency, accountability, and ethical standards?
10. What are the main types of corruption risks in corporate governance, and why do they need to be analyzed separately?
11. How does conflict of interest affect management decisions and increase vulnerability to corruption?
12. What internal control mechanisms (division of powers, monitoring, digital systems) are key to preventing corruption?
13. What compliance system failures led to corruption scandals at Rolls-Royce, Siemens, and Daimler, and what conclusions can Ukrainian companies draw from this?
14. Why does tolerating minor ethical violations eventually lead to systemic corruption?
15. Why can reputational damage be more devastating for a company than financial sanctions following a corruption incident?
16. What behavioral signals indicate a decline in corporate ethics and integrity within an organization?
17. Why is employee resistance to compliance requirements often linked to weak leadership or inconsistent management?
18. What approaches can be used to assess the maturity of an organization's compliance culture?
19. How does the dynamic nature of legislation at the national and European levels affect the compliance risk system?
20. Why do digitalization and the growth of cyber threats create additional risks for anti-corruption procedures and data protection?
21. What opportunities and risks does the integration of artificial intelligence into compliance processes create?
22. Why should compliance be integrated into strategic management rather than functioning in isolation?

23. How does a strong compliance system affect investment attractiveness and stakeholder confidence?
24. What organizational structures ensure an effective long-term ethical management system?

References for Self-study

1. Anti-corruption strategy for 2021-2025, approved by the Law of Ukraine dated June 20, 2022 No. 2322-IX "On the principles of the state anti-corruption policy for 2021-2025". URL: https://zakon.rada.gov.ua/laws/show/2322-20#Text
2. Companies' assessments of anti-corruption compliance, OECD 2025. URL : https://www.oecd.org/en/publications/companies-assessments-of-anti-corruption-compliance_977ed5a8-en.html
3. The Guardian: Rolls-Royce: SFO launches formal bribery and corruption investigation. URL: https://www.theguardian.com/business/2013/dec/23/rolls-royce-sfo-bribery-corruption-investigation-indonesia
4. Parsons,.Adam *(2017)* Rolls-Royce says sorry after corruption probe results in record fine. URL: https://news.sky.com/story/rolls-royce-says-sorry-after-corruption-probe-results-in-record-fine-10732589
5. Fuerst, M. J., & Luetge, C. (2021). The conception of organizational integrity: A derivation from the individual level using a virtue-based approach. Business Ethics, the Environment & Responsibility, Article beer.12401. Advance online publication, 32, 25–33. https://doi.org/10.1111/beer.12401
6. Fuerst, Madeleine J.; Luetge, Christoph; Max, Raphael; Kriebitz, Alexander (2023). Toward organizational integrity measurement: Developing a theoretical model of organizational integrity. URL: https://www.econstor.eu/bitstream/10419/288075/1/BASR_BASR12329.pdf
7. Fuerst, Madeleine J., Luetge, C. (2021)The conception of organizational integrity: A derivation from the individual level using a virtue-based approach. URL: https://onlinelibrary.wiley.com/doi/10.1111/beer.12401
8. Ferhani, Billel. (2025) Leadership and business ethics: a conceptual framework for responsible management. URL: https://virtusinterpress.org/IMG/pdf/cocv22i-1art9.pdf
9. Khrapkina, V.V.. Khrapkin, O.M. (2024). Rol lidera u formuvanni korporatyvnoi kultury pidpryiemstva. URL: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/b3d95c94-d15b-4b20-97d2-fc35105d98a6/content
10. Jensen, Michael C., Meckling William H. Theory of the firm: managerial behavior, agency costs and ownership structure. *Journal of financial economics*. 3 (1976) 305-360.
11. Press release. Daimler AG and Three Subsidiaries Resolve Foreign Corrupt Practices Act Investigation and Agree to Pay $93.6 Million in Criminal Penalties. URL: https://www.justice.gov/archives/opa/pr/daimler-ag-and-three-subsidiaries-

resolve-foreign-corrupt-practices-act-investigation-and

12. Liubimov, V.M. (2025). Antykoruptsiinyi komplaiens-menedzhment u systemi upravlinnia: orhanizatsiino-informatsiini aspekty [Anti-corruption management and system management: organizational and organizational aspects]. URL: https://www.inter-nauka.com/uploads/public/17405586019626.pdf
13. Perepelytsia, S. S. (2025). Kontseptualni zasady formuvannia kultury ta biznes-etyky orhanizatsii na zasadakh komplaiensu [Conceptual principles for forming an organization's culture and business ethics based on compliance]. URL: https://www.inter-nauka.com/uploads/public/17405586019626.pdf
14. Dietz, G., Gillespie, N. (2012). The Recovery of Trust: Case Studies of Organisational Failures and Trust Repair. URL: https://www.repman.com.tr/tr/wp-content/uploads/user/the-recovery-of-trust.pdf
15. The Guardian. (2012). Rebuilding trust: How Siemens atoned for its sins. URL: https://www.theguardian.com/sustainable-business/recovering-business-trust-siemens

Assignments for Self-Study

1. Essay (2 pages). Topic: The role of internal and external reporting channels in ensuring corporate integrity. Explain how internal and external reporting channels promote transparency and early detection of violations. Refer to ideas from the file material: the role of a leader, corporate ethics, internal control, risks of ignoring signals.
2. Mini-case (3–4 pages). Corporate response to whistleblower reports: analysis of an international case. Choose one case: Rolls-Royce, Siemens, Daimler AG, or another international/Ukrainian case. Describe how the organization responded to the report of the violation: were internal signals ignored; was an independent investigation conducted; were there sanctions, dismissals, changes in management structure. Suggest practices that could be adapted for Ukrainian companies, taking into account the Law of Ukraine «On Prevention of Corruption.»
3. Comparative table (1–2 pages). Comparison of EU standards for the protection of whistleblowers and Ukrainian anti-corruption legislation. Compare according to the following criteria: reporting channels (internal, external, public); anonymity and confidentiality; response and feedback times; protection from reprisals; role of independent bodies (ombudsman, NACP in Ukraine); requirements for employers. The table should: identify gaps in the Ukrainian system; provide suggestions on how to harmonize Ukrainian legislation with European legislation.
4. Interview reflection (1 page). Trust and psychological safety in reporting systems. Conduct a short interview with a representative of one of the following professions: compliance officer; internal auditor; lawyer; HR manager. Find out: what motivates/demotivates employees to report violations; how confidentiality is ensured; how management responds to the risk of reprisals; what typical fears

employees have. Write a 1-page reflection with an analysis of insights.

5. Practical task (2 pages). Draft internal policy on reporting violations. Develop a short policy that includes: terms (whistleblower, violation, good faith, reprisals); reporting channels (electronic form, hotline, external channels); confidentiality and anonymity rules; whistleblower protection; report review procedure; feedback deadlines; responsibilities of the manager and compliance officer.

Chapter 10: Evaluating the Effectiveness of a Compliance Management. Reporting

Learning Outcomes

After studying this chapter, learners will be able to:

- Understand the conceptual basis for determining the effectiveness of a compliance management system and the relationship between policies, risk management, monitoring, audits, and assessment results.
- Plan and implement monitoring and measurement, identify key performance indicators and key risk indicators (KRIs) to assess the effectiveness of compliance processes.
- Analyze assessment results and identify trends, causes of non-compliance, and systemic issues in the functioning of the compliance management system.

Key Words: performance evaluation, compliance management system, compliance, monitoring, measurement, analysis, audit, KPI (key performance indicators).

Main Definitions

Compliance Management System (CMS) – a set of policies, procedures, processes, and measures that help an organization comply with laws, regulatory requirements, standards, and ethical principles in its activities.

Compliance Management System Effectiveness Assessment – a comprehensive process of determining the level of effectiveness, adequacy, and efficiency of a compliance management system by analyzing, measuring, and monitoring its performance indicators in accordance with established criteria.

Effectiveness – the degree to which planned activities and achieved results correspond to the established goals of the compliance management system.

Standards, Laws, and Regulations

1. International: ISO 37302:2025 – Compliance Management Systems. Guidelines for Assessing Effectiveness, ISO 19011:2018 – Guidelines for Auditing Management Systems, ISO 31000:2018 – Risk Management. Guidelines, ISO 37000:2021 – Governance of Organizations. Guidance, ISO 37001:2016 — Anti-Bribery Management Systems, OECD Guidelines for Multinational Enterprises (оновлені у 2023 році), UN Global Compact (Глобальний договір ООН).

2. European Union (EU): EU Whistleblowing Directive (2019/1937/EU), EU Corporate Sustainability Due Diligence Directive (CSDDD, 2024), EU General Data Protection Regulation (GDPR, 2016/679), EU Directive 2014/95/EU (NFRD) / Corporate Sustainability Reporting Directive (CSRD, 2024).

3. Ukraine: Law of Ukraine "On Prevention of Corruption," Law of Ukraine "On Accounting and Financial Reporting in Ukraine," Tax Code of Ukraine, Law of Ukraine "On the Basic Principles of State Financial Control in Ukraine", National Agency for Corruption Prevention (NAZK) – Methodological recommendations for the implementation of anti-corruption programs.

List of Subchapters

10.1 Principles and objectives of assessing the effectiveness of a compliance system

10.2 ISO 37302:2025 Compliance management systems – Guidelines for assessing effectiveness

10.3 Methodology for assessing compliance management systems

10.4 System of indicators and scales for measuring the effectiveness of a compliance management system

10.5 Criteria and methods for assessing the effectiveness of a compliance management system

10.6 External confirmation and independent verification of the effectiveness of a compliance system

10.7 Continuous improvement of a compliance management system

10.1 Principles, objectives, and tools for assessing the effectiveness of compliance management systems

Among the leading scholars and practitioners who have made significant contributions to the development of the theory and methodology of assessing the effectiveness of compliance management systems, it is worth noting Soltes Eugene F., Joseph Zielinski, Mulugeta Bruke Mekuria, Michael Volkov, Todd Haugh, Klaus-Ulrich Remmerbach, Robin Krumme, Maximilian Jantz, Stephan Grüninger, Roland Müller, Daniel Lucien Bühr, Roland Maurhofer, Hans-Ulrich Westhausen, Ho-Pun Lam, and Mustafa Hashmi.

Soltes Eugene F. (2018) in his article "Evaluating the effectiveness of corporate compliance programs: Establishing a model for prosecutors, courts, and firms" notes that compliance effectiveness is assessed as a system rather than individual measures. He emphasizes the need to assess the integrity and consistency of compliance management. The assessment of compliance management consists of policies, culture, control, training, monitoring, incident management, etc. He points out that the significant financial and organizational resources that companies devote to compliance do not ensure the desired result due to the prevalence of formal ("paper-based") approaches that have no actual impact on employee behavior. He proposes a conceptual assessment model based on empirical data that allows determining the real effectiveness of compliance tools, such as hotlines for reporting violations,

training, disciplinary mechanisms, and analytical monitoring systems.

Joseph Zielinski in his article “The Effectiveness of Your Compliance Program” argues that the assessment of the effectiveness of a compliance program should be based on a three-pronged approach formulated in the US Department of Justice (DOJ) Guidance on the Evaluation of Corporate Compliance Programs. The main goal is to prove effectiveness, not just the formal existence of policies and procedures. He emphasizes that today’s regulators expect practical evidence of effectiveness, i.e., data, metrics, and analytics that show how the compliance system works, improves, and responds to risks. Joseph Zielinski’s (n.d.) main thesis: “The compliance department must have sufficient independence and appropriate resources.” Joseph Zielinski emphasizes that the modern approach to compliance goes beyond the formal existence of policies and procedures, focusing on actual performance results and the system’s ability to prevent violations. The assessment is based on three key DOJ questions: Is the compliance program well designed? Is it adequately resourced and independent? Does it work in practice? Six key blocks of system effectiveness assessment are revealed: risk management, policies and procedures, training, confidential reporting mechanisms, third-party control, and integration of compliance into M&A processes.

Mulugeta Bruke Mekuria (2016) in his article “Perceptions on an effective compliance management system” emphasizes that compliance cannot exist in isolation—it must be integrated with risk management, corporate governance, ethics, and internal control. Mulugeta Bruke Mekuria emphasizes that compliance is a systemic and strategic process, not a one-time task. The assessment of the effectiveness of a compliance management system should include: measuring the effectiveness of policies and training, analyzing incidents and staff behavior, and determining the level of risk and monitoring improvements. Mulugeta Bruke Mekuria argues that there is no universal model for measuring the effectiveness of a compliance system due to the diversity of business processes and regulatory conditions. He proposed a comprehensive approach that includes stakeholder surveys, competency analysis, expert assessments, audits of court and regulatory cases, and monitoring of corporate culture.

Liezl Groenewald and Guendalina Dondé (2017) emphasize in their guide to ethics and compliance that compliance should be value-based and ethical in nature, not just regulatory. They note that compliance is effective not where there are only rules, but where there is a culture of ethical behavior and responsibility, supported by an independent function, leadership support, a control system, and training. A company must build a value-oriented system where rules are the basis and ethical behavior is the strategic goal. They emphasize that although both systems are aimed at ensuring responsible behavior of personnel, their approaches differ significantly: ethics shapes the principles and values that should lead employees to “the right decisions,” while compliance ensures adherence to the organization’s legal and internal requirements.

Michael Volkov (2018) notes in his guide Ethics and the definition of successful companies. Corporate Compliance Insights that the effectiveness of compliance is determined by corporate culture. He emphasizes that assessing the effectiveness of the system cannot be limited to reviewing policies and procedures—the key criteria for

success are ethical employee behavior and the level of trust within the organization. “An ethical culture is the most effective compliance control... policies alone are insufficient.” He suggests: continuously measuring and analyzing corporate culture, including ethical KPIs in HR processes and personnel assessment, training through practical cases and ethical dilemmas, building a transparent system for responding to reports, and conducting regular analytics and reporting to the board of directors.

Todd Haugh (2018), in his article “The Power Few of Corporate Compliance,” argues that most companies build compliance on the assumption that violations are evenly distributed throughout the organization (normal distribution), so programs are focused on “broad coverage and uniform application.” Compliance programs mistakenly assume a “normal distribution” of violations and uniform risk. Hoá argues that corporate offences have a “fat-tailed distribution” — that is, most of the risk is concentrated in the actions of a small group of key individuals (“power few”). A small number of influential individuals can cause disproportionately large scandals and losses. It is necessary to study behavioral aspects—cognitive biases, social influence, network effects. Understanding behavioral ethics helps predict “extreme” violations, not just typical ones. Todd Haugh analyzed current approaches to assessing the effectiveness of compliance systems with a focus on behavioral aspects of risk and the concentration of violations in key groups of employees (“power few”).

Klaus-Ulrich Remmerbach and Robin Krumme (2020) noted in their article “The effectiveness of compliance management systems” that compliance effectiveness should be assessed using IDW AssS 980. They identify seven key components of an effective compliance system that should be evaluated: compliance culture, compliance objectives, compliance risk assessment, compliance program, compliance organization, communication and reporting channels, and monitoring and continuous improvement of the system. The compliance management system (CMS) should be assessed for compliance with the seven basic elements of IDW AssS 980. The study analyzes the effectiveness of compliance management systems (CMS) based on international standards and IDW AssS 980.

Gammisch Malcolm and Balina Signe (2014) in their article “The Effectiveness of Compliance Management Systems – An Experimental Approach” reveal the effectiveness of compliance management systems (CMS) based on an experimental study that models ethical dilemmas in a business environment. The results show that CMS have a positive effect on reducing the propensity for unethical behavior and corrupt practices. It has been established that the most effective components are information measures, control mechanisms, clear instructions, and reporting procedures, while sanctions have a limited impact. It has been proven that universal compliance programs are ineffective—measures must be targeted, precise, and adapted to the specific risks of the organization. The study emphasizes the role of ethical leadership and the need to foster an organizational culture of integrity as key factors in compliance effectiveness.

Hans-Ulrich Westhausen (2017) in his article “About the calculation of the compliance value and its practical relevance” argues that compliance is not only a legal obligation but also an investment that should be evaluated in monetary terms. “...the compliance function must be able to measure the quantified impact(s) ... and calculate the added

value and ROI of compliance." A significant gap has been identified in science and practice regarding the assessment of the economic effect of compliance. "The measurement of the compliance value is a 'blind spot'... in theory and practice." A systematic approach to calculating the value of compliance is proposed and a clear model is defined: compliance costs (one-off + ongoing), benefits/revenues (returns), calculation of added value (Value of Compliance) and ROI of compliance. To assess effectiveness, he suggests using: activity KPIs (trainings, audits), result KPIs (reduced losses, fewer fines), and behavioral metrics (ethics behavior indicators). "Activity, result, and behavioral-based compliance returns." Hans-Ulrich Westhausen identifies a "blind spot" in scientific research and corporate practice regarding the assessment of compliance benefits and proposes a systematic approach to monetizing results, including the classification of costs and benefits, the use of KPIs and behavioral indicators, and ROI calculation.

Ho-Pun Lam and Mustafa Hashmi (2020) in their article "A comparative study of compliance management frameworks: PENELOPE vs" note that compliance must be formalized and formally verifiable. The authors emphasize that the effectiveness of a compliance system depends on the organization's ability to formalize regulatory requirements, formally model norms and business processes, and perform a formal compliance assessment. "...lack of acceptable compliance tools and methodologies... raises the question of how to formally evaluate a CMF." Effective compliance should not only record violations, but also model: contrary-to-duty obligations, compensation mechanisms, and the possibility of repeated violations "compensated obligations... recursively violated and compensated again." Ho-Pun Lam and Mustafa Hashmi show that: PENELOPE better models temporal and procedural dependencies, PCL is more accurate in formalizing the logical structure of norms, and no framework is universal — a combinatorial model is needed to "determine the suitability of a CMF... for representing legal norms."

The International Organization for Standardization (ISO), the Organisation for Economic Co-operation and Development (OECD), the World Compliance Association (WCA), Transparency International, and the European Compliance and Ethics Institute (ECEI) play a significant role in standardizing the processes for assessing the effectiveness of compliance systems.

In particular, ISO 37301:2021 establishes requirements for compliance management systems, and the new ISO 37302:2025 standard provides specific guidance on methods for assessing the effectiveness of such systems. These documents define the key elements of assessment: monitoring, analysis, auditing, performance measurement, and continuous improvement.

In its Guidelines for Multinational Enterprises, the OECD outlines corporate governance principles based on transparency, accountability, and ethical behavior, which directly influence the assessment of compliance program effectiveness.

Transparency International examines the relationship between the effectiveness of compliance management systems and the level of corruption risks, emphasizing that a well-designed compliance system is a tool for preventing misconduct. In the 2023 Global Corruption Report, the Transparency International Secretariat (2023)

states that the effectiveness of a compliance management system (Compliance Management System, hereinafter CMS), it is stated that the effectiveness of a CMS is determined not by the number of policies, but by the extent to which the system: identifies key risks (corruption, tax, sanctions, AML, ESG), ensures their assessment, and implements control measures in accordance with the risks. The report states that "compliance is not a set of documents, but a system for managing the risks of violations." The report proposed a generalized system of indicators and metrics for assessing effectiveness, taking into account industry risks and international best practices.

In Ukraine, the issue of assessing the effectiveness of compliance management systems is only beginning to gain traction, but there are already a number of researchers developing related areas. Shvydka T. and Khaletska K. (2020) in their article "Compliance Control in the Corporate Governance System of Business Entities" note that the effectiveness of compliance is determined by the level of management involvement, transparency, continuity, and information openness. They believe that the assessment should include regulatory compliance, the quality of corporate governance, the presence of a compliance function, risk management, and integrity.

The main position of A. Khavanova (2025) in the article "Development and implementation of compliance indicators for assessing the maturity of the economic security system of enterprises" regarding the assessment of the effectiveness of the compliance management system is to determine effectiveness through the level of maturity of the system. Khanova A. emphasizes that compliance assessment should be based on a maturity model with detailed levels of development — from basic to leadership. She proposed a five-level maturity model and a system of indicators grouped by functional blocks: organizational and managerial, regulatory and legal, monitoring, educational and cultural, and innovative and digital, which will allow assessing the degree of institutionalization of the function, the depth of integration into management, as well as the adaptability and innovativeness of the system. She defined a scoring scale for indicators and the possibility of adapting weights depending on industry risks and the scale of the enterprise. Kavanova A. noted that the assessment results are aggregated into an integral index, which allows identifying strengths and weaknesses, building a risk map, planning system improvements, and conducting benchmarking between enterprises.

O. Okunev, O. Shenk, and others (2023) in the guide "Anti-Corruption Compliance" emphasize that effective compliance is determined by the ability to identify and manage corruption risks, implement preventive measures, and support from management. They argue that an effective compliance system is based on a risk-oriented approach, an active role of management ("tone at the top"), the existence of internal policies and procedures, the functioning of an independent compliance function, and the implementation of mechanisms to prevent, detect, and respond to violations. They emphasize the importance of a corporate culture of integrity, staff training, reporting and whistleblower protection procedures, systematic monitoring, and auditing. They determine that the key criterion for assessment is the practical effectiveness of the compliance system, rather than its formal existence. They

propose a system of assessment indicators adapted to international standards (ISO 37301, ISO 37001) and the Ukrainian regulatory environment.

Sagaidak M.P., Marynyuk I.O. (2024) in the article “Research on the theoretical foundations of the formation of a compliance management system for organizations” emphasize that the effectiveness of compliance depends on its implementation in the management system. They emphasize the need to build an integrated compliance system that combines policies, procedures, internal audit, and cultural and value components. They highlight the difference between “formal” and ‘real’ compliance, noting the risks of “compliance on paper,” and prove the importance of practical implementation of standards.

Gura V. (2023) in the article “Compliance system as a way to overcome corruption” considers compliance as an integrated system of compliance with legislation, ethical standards, and internal procedures. She notes that effectiveness is achieved through the independence of the compliance department, staff training, monitoring, ethical culture, and control systems. She argues that compliance increases economic security, stakeholder trust, and corporate reputation.

Thus, contemporary research shows that the effectiveness of a compliance management system is determined not only by formal compliance with standards, but also by the level of integration of ethical principles, a culture of trust, and transparency into the organization’s activities. International standards ISO 37301 and ISO 37302 serve as a methodological foundation, while the scientific approaches of leading researchers provide practical tools for evaluating and improving compliance systems.

Monitoring, measurement, analysis, and evaluation are strategic compliance management tools (Figure 10.1) that ensure: evidence of the effectiveness of the compliance management system, timely identification and minimization of non-compliance risks, the formation of a culture of transparency and integrity, a focus on results rather than formal compliance with procedures, and continuous improvement of the system in accordance with ISO 37302:2025.

Figure 10.1 Compliance management system monitoring, measurement, and evaluation cycles

The cycle of monitoring, measurement, analysis, and evaluation forms a closed management system. Each stage forms the basis for the next, providing feedback for management decisions, adaptability of the system to changes in the external environment, and its continuous improvement in accordance with the requirements of ISO 37302 and ISO 9004.

The results of the monitoring and evaluation processes should be documented in the form of: reports on the effectiveness of the compliance management system, recommendations for improvement, updated risk maps and control plans, and

management decisions on changes to compliance policies, resources, or objectives.

Monitoring is the systematic observation and verification of the functioning of the management system to determine whether the system is working as planned and whether it complies with the requirements of legislation, corporate policies, and ethical standards.

The main tasks of monitoring include tracking compliance obligations, controlling the effectiveness of procedures, policies, and internal controls, identifying violations, incidents, and areas of risk, and generating data for further analysis and measurement. The types of monitoring and their specific features are shown in Figure 10.2.

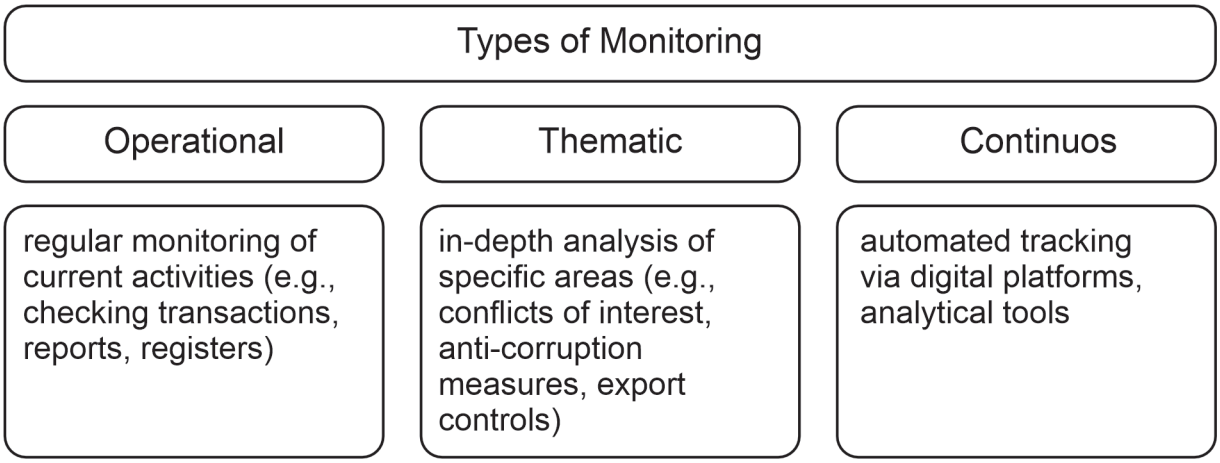


Figure 10.2 Types of monitoring

Monitoring tools can include compliance event logs, compliance reporting tools, software for tracking risks and control indicators, and periodic internal audits and policy reviews.

The effectiveness of the compliance management system can be measured using a quantitative or qualitative assessment of the system's performance based on specific indicators, such as:

1. KPI (Key Performance Indicators) – key performance indicators (e.g., % of compliance training plans completed).

2. KRI (Key Risk Indicators) – key risk indicators (e.g., number of incidents reported).

3. PI (Process Indicators) – indicators of the effectiveness of individual processes (e.g., average response time to reports of violations).

The purpose of measuring the effectiveness of a compliance management system is to confirm that its objectives have been achieved, evaluate the effectiveness of processes, and build an evidence base for improving the system.

Analysis can be used to interpret the data obtained during monitoring and measurement in order to identify trends, patterns, and problem areas in the operation of the

management system. The main tasks of such analysis are to assess the dynamics of non-compliance risks, identify systemic deficiencies in procedures, predict possible incidents, and form a basis for strategic decisions and corrective actions.

Methods of analysis:

- Quantitative analysis: statistical reports, comparative tables, deviation analysis.
- Qualitative analysis: expert assessments, content analysis of documents, staff surveys.
- Comparative analysis (benchmarking): comparison of results with best practices or external standards (ISO 37302, ISO 37001, ISO 31000).
- Correlation analysis: identifying relationships between factors (e.g., between staff training levels and the number of incidents).

Management system assessment includes a comprehensive review of the effectiveness of the compliance management system, aimed at determining the degree to which objectives have been achieved, compliance with requirements, and opportunities for improvement.

Typical approaches to management system assessment are self-assessment: performed by an internal compliance officer, internal audit: verification of compliance with ISO 37301 requirements, and effectiveness review: in accordance with ISO 37302:2025, includes verification of the achievement of objectives, the effectiveness of processes, and the maturity of the compliance culture.

10.2 Assessing the effectiveness of a compliance management system in accordance with ISO 37302:2025

ISO 37302:2025 is a logical extension of ISO 37301:2021 and provides guidance on assessing the effectiveness of compliance management systems. Its purpose is to provide organizations with a systematic, evidence-based, and measurable approach to assessing the functioning of their CMS, enabling them to improve its effectiveness, consistency, and sustainability.

The standard does not contain mandatory requirements, but is a guideline that helps organizations: assess the effectiveness of existing compliance management processes; identify weaknesses in the system; implement mechanisms for continuous improvement; ensure transparency and accountability to stakeholders.

The ISO 37302:2025 standard, “Compliance management systems – Guidance for the evaluation of effectiveness,” can be structured as follows:

1. Principles for evaluating the effectiveness of a compliance management system. ISO 37302 establishes the fundamental principles that should be taken into account when analyzing and evaluating the system:

- > systematicity, i.e., evaluation not only of procedures, but of the entire CMS;
- > outcome orientation – not only the performance of formal actions;
- > evidence-based – the presence of measurable indicators;
- > continuous improvement - assessment should lead to change and development.

2. Framework of indicators and criteria (indicator framework). The standard proposes a system of indicators by which an organization can measure the effectiveness of the CMS - both quantitative and qualitative. It also provides criteria for their assessment: what data to collect, how to interpret it, how to compare it with baseline levels.

3. Assessment process The standard contains guidelines on the stages of effectiveness analysis: planning, information gathering, measurement, analysis, reporting, and improvement.

4. Maturity model and approaches to interpretation ISO 37302 provides for the use of scales (maturity levels) or ratings that allow an organization to place its CMS on a "scale" of development - from initial to optimized.

The ISO 37302 standard does not change the requirements set out in ISO 37301:2021 (Requirements for compliance management systems), but supplements them - it helps to measure how well the system is working. This means that if you already have a compliance management system in accordance with ISO 37301, ISO 37302 will be the next step in assessing its effectiveness.

The main areas to be assessed under the standard include: policies, procedures, and controls; behavior and compliance culture; results and impact (including on business operations, reputation, and compliance); monitoring, analysis, reporting, and corrective actions. (According to analysts: indicators cover "Policy & Procedures," "Conduct & Culture," "Results & Impacts").

It is important to note that the standard is not certification-based, i.e., an organization cannot obtain a certificate specifically for ISO 37302. It does not change existing requirements and is focused solely on assessing effectiveness. It is suitable for different types of organizations and can be scaled according to size, industry, and risk level.

In accordance with the requirements of ISO 37302, the assessment of a compliance management system is based on the following principles:

1. Objectivity - the use of independent, verified evidence to confirm the results of the assessment.
2. Systematicity - assessment of the entire CMS, including policies, processes, controls, culture, and behavior.
3. Proportionality - adaptation of approaches and criteria to the size, context, and risks of the organization.
4. Continuous improvement - assessment is not a one-time event, but part of the PDCA (Plan–Do–Check–Act) cycle.

5. Outcome-based evaluation - measuring not only the existence of processes, but also the actual achievement of compliance objectives.

The practical significance of applying this standard for organizations is that the organization obtains a structured approach to not just “being compliant,” but to demonstrate effective compliance, can be used as a basis for building a system of KPIs and compliance indicators that measure not only the process but also the result, assists in reporting to stakeholders – investors, regulators, internal managers – and supports the continuous improvement of the compliance management system through regular assessment and adjustment.

ISO 37302:2025 is an important step in the development of compliance management system standardization. It bridges the gap between the formal implementation of compliance mechanisms (through ISO 37301) and the measurement of their actual effectiveness. For organizations wishing to move from “compliance” to “achieving results,” this standard provides clear methodological support.

10.3 Methodology for assessing compliance management systems

The methodology for assessing compliance management systems defines the principles, approaches, sequence of stages, and methods used to measure the effectiveness, efficiency, and maturity of a compliance management system (CMS). It ensures the systematic, evidence-based, and consistent nature of the assessment process, allowing the organization not only to verify compliance with requirements, but also to continuously improve its compliance culture and increase its resilience to non-compliance risks.

The main purpose of compliance management assessment is to confirm the extent to which the compliance management system effectively ensures compliance with legislative, regulatory, contractual, and internal requirements, as well as its ability to prevent, detect, and respond to incidents of non-compliance.

The key tasks of the assessment include:

- verifying the existence and adequacy of policies, procedures, and controls;
- assessing the effectiveness of control mechanisms in actual operations;
- identifying gaps and risk areas;
- analyzing the level of compliance culture and staff awareness;
- formulating recommendations for improvement (Corrective and Preventive Action - CAPA) and determining their priority.

Compliance Assessment is a systematic analysis process that determines how effectively an organization ensures compliance with legal, ethical, internal, and international requirements, as well as the maturity of its compliance culture (Figure 10.3).

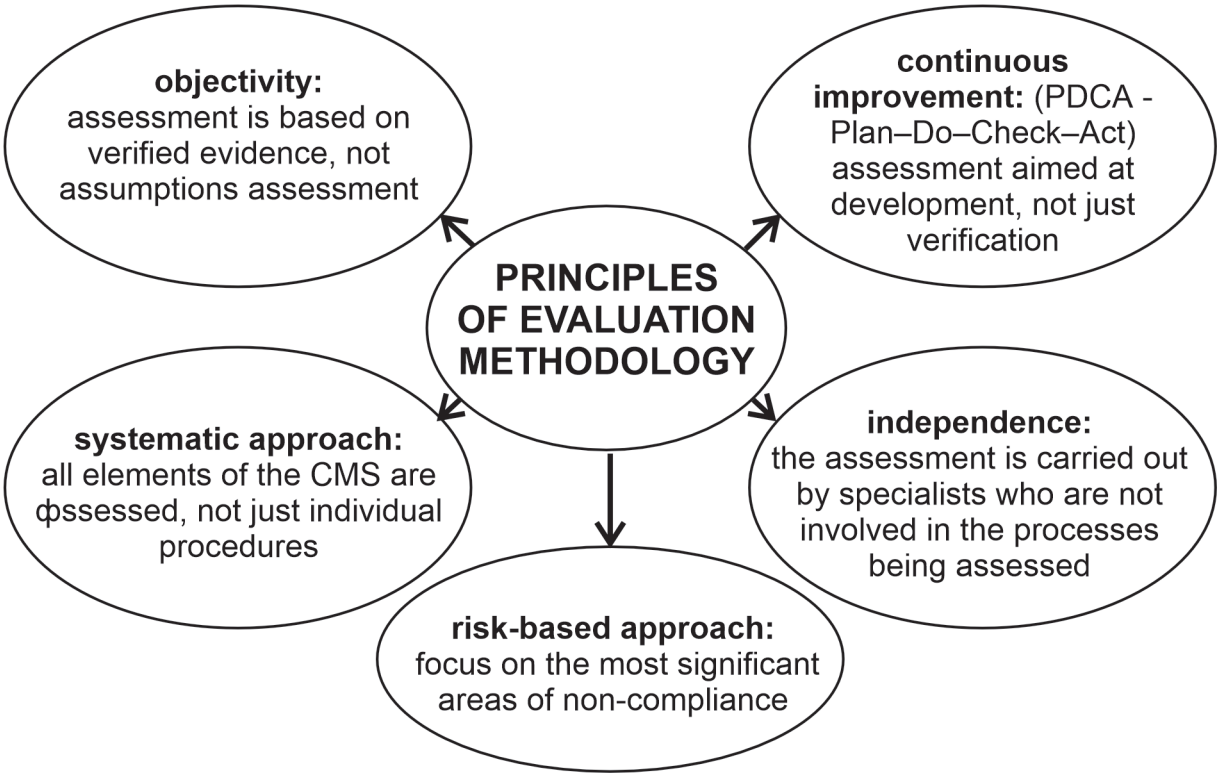


Figure 10.3 Basic principles underlying the assessment methodology

The methodology involves conducting an assessment in five main stages. ISO 37302 offers the following staged model for assessing the effectiveness of a compliance management system.

The first stage is preparatory (assessment planning). The purpose of this stage is to define the scope, criteria, and methods for assessing the CMS. At this stage, an assessment working group is formed, which may include internal auditors, compliance officers, and independent experts. The objects of assessment must be defined; they may include individual departments, individual processes, policies, and programs. In addition, assessment criteria are agreed upon in accordance with ISO 37301, internal policies, and legal regulations, and an assessment program and work schedule are developed. The result of the first stage is an assessment plan with defined deadlines, resources, and data collection methods.

The second stage is the identification and analysis of non-compliance risks. At this stage, the context of the organization's activities and its compliance risks are assessed. An analysis of the external environment (legislative changes, regulatory requirements) is carried out, and internal factors are assessed, including organizational structure, corporate policy, and previous incidents. At this stage, key areas of non-compliance are identified and a register of compliance risks is formed, indicating their probability and impact. The result of the second stage is a Compliance Risk Matrix, which is the basis for further assessment.

The third stage is the collection and analysis of evidence. This collection is performed using a combination of qualitative and quantitative methods. At this stage, evidence collection methods such as document analysis (policies, codes of ethics, reports, audit reports), interviews and surveys (employees, management, external partners), observation of compliance measures, audits and testing of control mechanisms, and assessment of KPIs, namely: frequency of incidents, level of training, implementation of recommendations, etc. The main result at this stage is the formation of a factual database for assessing the maturity and effectiveness of the system.

The fourth stage is effectiveness assessment (measurement and interpretation of results). At this stage, the actual state of the system is compared with the reference criteria. The following methods are used to assess effectiveness:

- the first method is a scoring model, i.e., each criterion is assigned a level: low (1), medium (2), high (3);
- the second method is weighted scoring, i.e., different criteria are weighted according to their importance (e.g., risk management = 30%, training = 15%);
- the third method is benchmarking, i.e., a comparison with the best global practices is made;
- the fourth method is expert assessment, involving internal and external experts to assess the maturity of the CMS.

The main result at this stage is the determination of the Compliance Maturity Index (CMI) in percentage or point terms.

The fifth stage is the formation of conclusions and an improvement plan. At this stage, a CMS assessment report (Compliance Assessment Report) is prepared, the identified strengths and weaknesses of the system are summarized, a corrective and preventive action plan (CAPA) is developed, and indicators for monitoring improvements in future periods are determined. The main result at this stage is a practical document that allows management to make informed decisions about improving the CMS.

The results of the methodological process are:

- CMS maturity level (Initial / Developing / Established / Advanced / Optimized);
- efficiency index (in % or points);
- profile of the system's strengths and weaknesses;
- recommendations for improving policies, procedures, training, and monitoring.

The methodology for assessing compliance management systems is not only a control process, but also a tool for strategic risk and reputation management of the organization. It allows you to identify gaps in the control system, determine the level of corporate maturity, and ensure continuous improvement of compliance in accordance with international requirements and ethical standards.

10.4. System of indicators and scales for measuring the effectiveness of the compliance management system

An effective compliance management system not only records incidents, but also assesses the effectiveness of preventive measures, the level of staff awareness, and management responsibility. The effectiveness of the management system is measured using indicators such as KPIs (Key Performance Indicators) (e.g., % of compliance training plans completed), KRIs (Key Risk Indicators) (e.g., number of incidents reported), and PIs (Process Indicators) (e.g., average response time to reports of violations).

KPI (Key Performance Indicators) – key performance indicators (e.g., % of compliance training plans completed). These indicators allow assessing the effectiveness of implemented compliance procedures, the level of compliance with policies, standards, and ethical principles, the degree of integration of compliance into strategic management, and progress in improving the compliance culture (Table 10.1). Key Performance Indicators (KPIs) must comply with the SMART principles: Specific – clearly defined what is being assessed; Measurable – has a quantitative or qualitative value; Achievable - achievable (realistic goals); Relevant - relevant (related to the goals of the compliance system); Time-bound - time-bound (clear assessment periods).

Table 10.1 List of key performance indicators for the compliance management system

Groups of Key Performance Indicators	Indicator
Strategic KPIs reflect the alignment of the CMS with corporate strategy and principles of good governance	Compliance Maturity Index
	Alignment with ESG/SDG goals (Sustainable Development Goals)
	Frequency of compliance policy reviews
Organizational KPIs assess risk management processes, documentation, communication, and training	Training Coverage Rate
	Share of officials covered by risk assessment
	Average incident response time
	Level of documented procedures
Behavioral KPIs focus on the culture of ethical behavior and employees' willingness to comply with policies	Ethics Culture Index
	Number of whistleblowing reports
	Rate of repeated violations
Operational KPIs measure the effectiveness of current procedures and controls	Frequency of internal audits
	Number of corrective actions
	Share of implemented audit recommendations
	Share of minor non-conformities

Reputational and Analytical KPIs	Number of external inspections without violations
	Reputation Risk Index
	Number of compliance-related disclosures in company reports

KPI measurement is carried out by collecting data from responsible persons (compliance department), HR, and internal auditors. Sources of information include internal databases, surveys, reports, and incident logs.

Key risk indicators (KRIs) are quantitative or qualitative parameters that reflect the likelihood of non-compliance risks or their consequences for the organization. Their purpose is to signal problems in the CMS in a timely manner before they turn into actual violations or losses (Table 10.2).

KRIs in a compliance system help to: measure risk appetite and risk tolerance; track trends in violations; assess the effectiveness of controls; support management decision-making based on risk analytics.

Table 10.2 Classification of key risk indicators in the compliance management system in accordance with ISO 37302 requirements

Risk Category	Characteristic	Examples of KRIs
Legal and regulatory risks	Violations of legislation, licensing requirements, or standards	– Number of regulatory changes not followed by policy updates – Share of overdue legal reports – Number of regulatory fines
Corruption risks	Risks of bribery, abuse, and conflicts of interest	– Number of identified conflicts of interest – Share of transactions conducted without due diligence – Number of anti-corruption investigations
Financial compliance risks	Risks of fines, sanctions, and financial losses caused by non-compliance	– Amount of financial sanctions over the period – Share of transactions without documentary support – Percentage of overdue tax reports

Reputational risks	Risks of losing the trust of partners, clients, and society	– Number of negative media mentions – Employee trust index in ethical policy – Number of internal complaints about unethical behavior
Operational risks	Risks associated with errors in processes, procedures, or IT systems	– Share of deviations in procedure execution – Number of technical failures in the compliance system – Incident response time

Integration of KRI into the CMS performance assessment process:

1. Determination of risk appetite – management approves acceptable KRI thresholds.
2. Real-time monitoring – a control panel (Compliance Risk Dashboard) is created.
3. Trend analysis – conducted quarterly to forecast future risks.
4. Link to KPIs – KRIs are integrated with performance indicators (for example, a high KRI automatically lowers the KPI rating).
5. Corrective actions – KRI results form an action plan within the PDCA (Plan–Do–Check–Act) cycle.

These indicators are assessed according to the relevant scale (Table 10.3).

Table 10.3 Scale for assessing key risk indicators in the compliance management system

Level	Interpretation	Range (%)	Signal
1	Very low risk	0–20	The system is stable
2	Controlled risk	21–40	Ongoing monitoring
3	Moderate risk	41–60	Requires analysis
4	Increased risk	61–80	Immediate action required
5	Critical risk	81–100	Crisis zone

The Key Risk Indicator (KRI) system makes it possible to transform risk-based thinking into a measurable practice, ensure the early detection of problems within the compliance management system, integrate risks into managerial decision-making, and enhance the overall maturity of the compliance management system to ISO 37301 Level 4–5.

Table 10.4 List of Key Performance Indicators for the Processes of the Compliance Management System

Process	Objective	Examples of Indicators
Compliance risk management process	To ensure the identification, assessment, and mitigation of risks related to violations of legislation or ethical standards	– Percentage of identified risks for which response plans have been developed (%) – Share of risks reviewed within the established timeframes (%) – Number of incidents related to delayed risk assessment – Average response time to an identified risk (days) – Share of risks reassessed after changes in business processes
Training and awareness-raising process	To ensure an adequate level of employee knowledge regarding compliance requirements	– Percentage of employees who have completed mandatory training (%) – Number of training hours per employee – Level of test results after training (% average score) – Share of employees who demonstrated improved knowledge based on repeated assessment (%)
Communication and reporting process	To ensure openness, transparency, and effective information exchange	– Number of internal messages or newsletters on compliance issues – Level of employee awareness of channels for reporting violations (%) – Average response time to compliance-related inquiries – Number of reports to management on compliance with compliance policies

Incident management process (compliance violations)	To promptly detect, investigate, and eliminate the causes of non-conformities	– Number of registered compliance incidents over the period – Percentage of incidents resolved within the established timeframe (%) – Average incident investigation time – Share of repeated violations (indicator of the effectiveness of preventive actions) – Number of disciplinary or corrective measures implemented after investigation
Monitoring, measurement, and audit process	To assess the extent to which the system fulfils its tasks and complies with ISO 37301 requirements	– Number of internal audits conducted according to the plan (% of plan completion) – Share of identified non-conformities eliminated within the established timeframe (%) – Number of repeated non-conformities (indicator of the sustainability of changes) – Number of recommendations implemented based on audit results.
Policy and procedure management process	To ensure the relevance, consistency, and practicality of normative documents	– Share of policies reviewed within the established timeframe (%) – Number of outdated documents in the system – Number of changes introduced following audit results or risk assessment – Level of user satisfaction with the usability of policies (based on a survey)

External review process	To ensure compliance with the requirements of regulators, partners, and standards	– Number of remarks or sanctions issued by regulatory authorities – Share of compliance reports submitted on time (%) – Rate of positive results of external audits (%) – Number of certification non-conformities requiring corrective action.

It is recommended to use a rating scale of 1–5 for each KPI (Table 10.5).

Table 10.5 Rating scale for key performance indicators of compliance management system processes

Level	Performance Description	Example Interpretation
1	Low	The system does not achieve its objectives and there are high risks of violations.
2	Limited	Processes exist, but they are fragmented.
3	Moderate	The system operates steadily, but without analytical control.
4	High	Processes are optimized and indicators exceed the required standard.
5	Excellent	Processes are integrated into strategic management.

Key performance indicators for individual CMS processes ensure systematic monitoring, accountability, and transparency. Regular analysis of these indicators helps identify weaknesses in compliance management, assess progress in achieving compliance goals, provide evidence for internal and external audits, and promote continuous improvement of the compliance management system in accordance with ISO 37301 and ISO 37302 requirements.

10.5. Criteria and methods for evaluating the effectiveness of the compliance management system

An effective compliance management system (CMS) must be based on clearly defined criteria that allow for an objective assessment of its effectiveness, maturity, and adaptability. Such criteria reflect a comprehensive combination of organizational, ethical, legal, and strategic aspects of the enterprise's activities.

The assessment of the effectiveness criteria of a compliance management system (CMS) is based on the principles of ISO 37301:2021, ISO 37001:2016, COSO, and internal audit practices (IIA) (Table 10.6).

Table 10.5 Assessment of the effectiveness criteria of a compliance management system (CMS)

Assessment Criterion	Description of the Criterion	Indicators / KPIs	Maturity Level (Low – Medium – High)
Compliance with legislation and standards	The degree to which the system complies with the requirements of ISO 37301, ISO 37001, national laws, and internal policies	Share of policies aligned with standards; number of non-conformities identified during audits	**Low:** lack of a systematic approach; **Medium:** partial compliance; **High:** full implementation of standards
Leadership and corporate culture	The activity of leadership in promoting ethical values and principles of integrity	Existence of a code of ethics; regularity of management compliance reports; staff surveys	**Low:** reactive management; **Medium:** policies exist but are not integrated; **High:** strong culture of integrity
Identification and management of compliance risks	The systematic nature of identifying, assessing, and monitoring compliance risks	Existence of a risk register; frequency of risk map updates; use of ISO 31000	**Low:** fragmented risk management; **Medium:** basic risk map; **High:** integrated risk management system

Policies, procedures, and control mechanisms	The degree of formalization and effectiveness of internal policies and procedures	Number of documented procedures; results of compliance checks; employee feedback	**Low:** absence of a policy system; **Medium:** processes are partially described; **High:** up-to-date and effective policies
Training and awareness	The existence of a system for employee training and the development of a compliance culture	Number of training sessions conducted; % of staff who completed training; level of knowledge based on test results	**Low:** one-off training sessions; **Medium:** regular training; **High:** continuous knowledge development programme
Monitoring, audit, and reporting	The effectiveness of control, audit, and reporting on compliance issues	Frequency of internal audits; number of reports; % of implemented recommendations	**Low:** absence of reporting; **Medium:** periodic reviews; **High:** regular audits and transparent reporting
Incident response and disciplinary measures	The timeliness of response to violations and the implementation of preventive measures	Average response time; number of repeated incidents; investigation results	**Low:** reactive actions; **Medium:** partial response; **High:** systematic incident management
Continuous improvement	The existence of processes for analysis, self-assessment, and updating of the CMS	Frequency of policy reviews; number of improvements implemented; benchmarking results	**Low:** no changes; **Medium:** improvements made as needed; **High:** strategic system improvement

Compliance with regulatory requirements and standards is a fundamental criterion that reflects the degree of compliance of the system with applicable legislation, internal policies, and international standards. The compliance of the structural elements of the system with the principles of ISO 37301:2021 (context, leadership, planning, support, operational activities, performance evaluation, improvement), the implementation of anti-corruption mechanisms in accordance with ISO 37001:2016, and compliance with the principles of good governance and the COSO Internal Control framework.

Leadership and corporate culture are criteria used to determine the level of management involvement in ensuring compliance and are key indicators of the system's sustainability. Criteria include the presence of a clear "tone at the top," the creation of an ethical corporate culture that encourages openness and prevents violations, and management participation in regular reviews of policies and compliance results.

Identifying, assessing, and managing compliance risks is a key criterion that shows how mature a risk management system is. The assessment criteria are the existence of a register of compliance risks, the use of risk-based methods (in accordance with ISO 31000:2018), the frequency and depth of monitoring of control measures, and the effectiveness of response plans for violations.

Policies, procedures, and control mechanisms are criteria for assessing the quality of formalizing compliance processes and determine their stability. The presence of internal codes of ethics, due diligence procedures, anti-corruption rules, the effectiveness of whistleblowing channels and documentation, transparency, and traceability of compliance processes are assessed.

Training, awareness, and communication are criteria for assessing a compliance management system, which must be integrated into corporate culture through training and communication and determines the frequency and quality of compliance training, the level of staff awareness of ethical standards, and the effectiveness of information channels for disseminating compliance policies.

Monitoring, auditing, and reporting are criteria for evaluating a compliance management system, as its effectiveness is impossible without verifying the effectiveness of control mechanisms, which involves assessing the regularity of internal and external audits, the functioning of a system of performance indicators (KPIs/metrics), and the transparency of reporting on incidents, audit results, and corrective actions.

Incident response and corrective actions are an assessment criterion that covers the existence of procedures for investigating non-compliance incidents, the speed and adequacy of corrective actions, and the effectiveness of mechanisms to prevent repeat violations.

Continuous improvement, in accordance with ISO 37301, involves the ongoing development of the compliance management system. This criterion assesses the existence of processes for monitoring and evaluating effectiveness, implementing corrective measures, and integrating audit results and feedback into planning and the use of digital tools for risk analysis.

Table 10.7 Compliance management system effectiveness criteria assessment scale (points)

Maturity Level	Description	Score (Points)
Low	The system is unstructured and lacks clear policies and control mechanisms.	1 point
Medium	The system is partially implemented but requires further improvement of procedures and controls.	2 points
High	The system fully complies with international standards, operates effectively, and demonstrates sustainable results.	3 points
Overall effectiveness of the CMS = total score for all criteria / maximum possible score × 100% Effectiveness levels: > up to 50% - the system requires substantial development; > 51–75% - the system is operational but requires further improvement; > above 75% - the system is effective and mature.		

A consolidated assessment of compliance management system effectiveness criteria can be used as a tool for diagnosing its maturity in analytical studies, reports, or audits.

The criteria for assessing compliance management systems should reflect a balance between formal requirements, practical effectiveness, and the development of a corporate culture of integrity. The most mature systems are those that combine legal precision, ethical awareness, and flexibility in adapting to new regulatory challenges.

ISO 37302 provides a flexible approach to defining performance evaluation criteria that can be adapted to the context of the organization (Table 10.8).

Table 10.8 - Main groups of performance evaluation criteria

Assessment Area	Examples of Criteria	Possible KPIs
Policy and governance	Existence and up-to-dateness of the compliance policy; clarity of roles and responsibilities	% of updated policies; number of training sessions for management
Compliance processes	Timeliness of risk identification; adequacy of monitoring procedures	Number of identified / resolved violations; % of implemented measures

Compliance culture	Staff awareness; participation in training; reporting of violations	Level of engagement; number of ethical reports
Performance Achievement of compliance objectives; reduction in the number of incidents Trend in the reduction of violations; improvement in reputation rating		
Improvement	Implementation of action plans based on audit results	% of implemented recommendations; incident response time

ISO 37302:2025 establishes a new paradigm for assessing the effectiveness of compliance management – from checking formal procedures to measuring actual results. This standard enables organizations to quantitatively assess the maturity of their CMS, obtain evidence for management decisions, improve corporate accountability culture, and ensure long-term sustainability and trust from regulators and society.

The standard provides for the use of different methods depending on the objectives and scope of the assessment (Figure 10.4); their characteristics are presented in table 10.9.

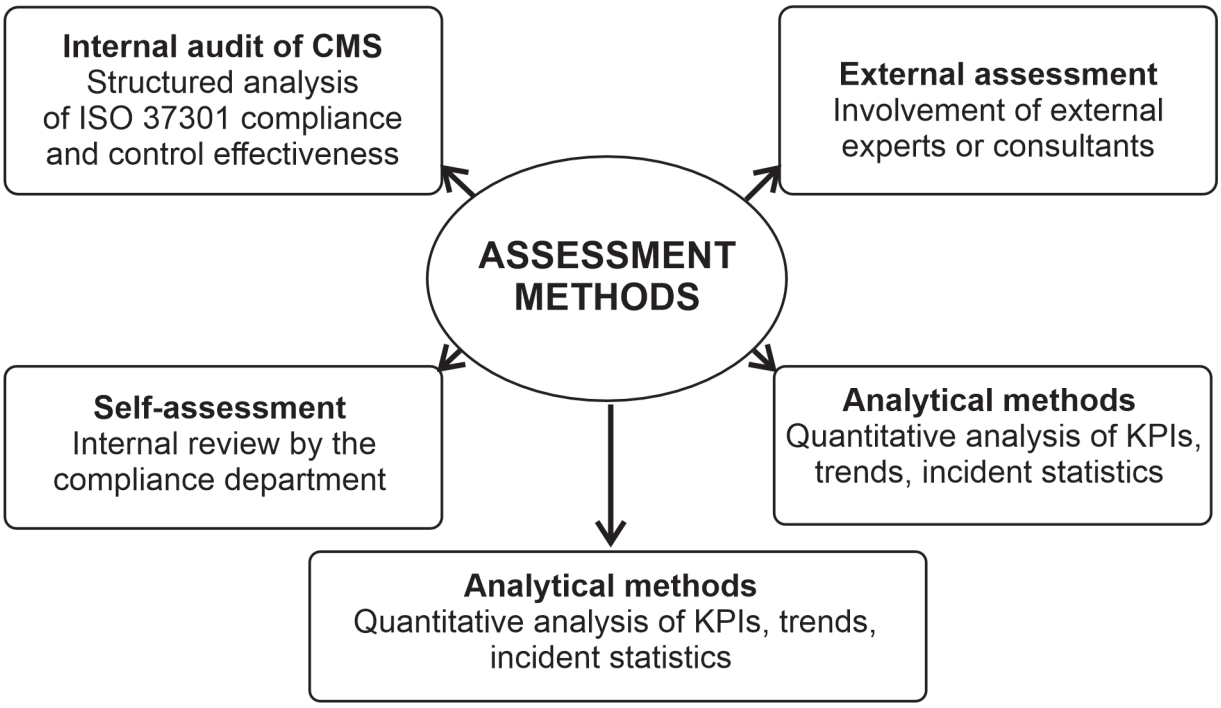


Figure 10.4 - Assessment methods

Table 10.9 Characteristics of assessment methods

Method	Characteristic	Advantages
Compliance Assurance Engagement	Independent assessment of whether policies and processes comply with established requirements	Objectivity, evidence-based results, suitability for certification
Self-Assessment	Internal analysis conducted by the compliance unit or management	Flexibility, low cost, rapid feedback
Peer Review	Assessment carried out by independent specialists or industry experts	Depth of analysis, industry benchmarking
Questionnaires and Surveys	Collection of data on the level of awareness, ethical culture, and attitudes towards compliance	Measurement of “soft” cultural indicators
Quantitative KPI Assessment	Use of key indicators (number of violations, training sessions, audits, etc.)	Enables monitoring over time

The first method is internal compliance auditing. It is carried out by the internal audit service or an independent compliance unit. The aim is to assess compliance with policies, procedures, and regulatory requirements. The methodological basis is the International Standards for the Professional Practice of Internal Auditing (IIA).

The second method is self-assessment. The organization independently diagnoses its compliance management system using control questions or a compliance maturity model. This method allows you to quickly identify weaknesses in the system and plan improvements.

The third method is assessment for compliance with the ISO 37301 standard. A certification audit by an independent body assesses the extent to which the system complies with the requirements of ISO 37301. The result is either certification or a report listing non-conformities for elimination.

The fourth method is compliance risk assessment. This method involves identifying, analyzing, and ranking the risks of non-compliance with legal, ethical, or contractual requirements. The toolkit is based on ISO 31000 and COSO ERM.

The fifth method includes analytical methods (KPI and Data Analytics). Quantitative indicators are used – frequency of violations, costs of eliminating non-compliance, number of disciplinary cases, etc.

Data analysis allows for an objective assessment of the effectiveness of policies and the timeliness of management actions. Benchmarking is used to compare your own compliance management system with the best industry or international practices.

This allows you to determine the maturity level of the system and form a development plan.

Effective assessment of compliance management systems is not only a control tool, but also a mechanism for continuous improvement of corporate governance. The use of a combination of methods – internal audit, certification, self-assessment, risk analysis, and KPIs – provides a comprehensive, objective picture of the state of the compliance system (Table 10.10).

Table 10.10 Methods and techniques for assessing the effectiveness of compliance management systems

Method Name	Essence
Documentary Analysis	Verification of the existence and completeness of the organization's regulatory framework: compliance policy, code of ethics, anti-corruption provisions, risk management procedures, registers of violations, and training records.
Interviews and Focus Groups	Used to collect qualitative data on the practical implementation of policies and employees' perception of the compliance culture.
Staff Surveys (Questionnaires)	The purpose is to identify the level of awareness, engagement, and willingness to report violations.
Control Testing	Design testing – analysis of the adequacy of control design. Operational testing – verification of the actual functioning of controls.
Analytical Methods (Data Analytics)	Use of digital analytics to detect violations: identification of anomalous transactions, analysis of access logs, detection of potential conflicts of interest, and verification of third-party compliance.
Comparative Analysis (Benchmarking)	Comparison of the existing compliance management system with international standards or industry practices (ISO 37301, ISO 37001, COSO, OECD Guidelines).
Self-Assessment	Involvement of internal units in assessing their own processes through standardized questionnaires or checklists.
Audit Approach	Application of internal audit principles - independence, evidence-based assessment, systematic approach, and objectivity - in evaluating CMS effectiveness.

Maturity models are an assessment of CMS through maturity levels (e.g., from “initial/reactive” to “optimized/preventive”), the criteria for which are policies, processes, technologies, people, KPIs, and integration with risk management.

Compliance management system assessment is a comprehensive, multi-point process that should be based on a risk-oriented approach, evidence-based methodology, and a combination of classic techniques (audits, interviews) with modern ones (data analytics, process mining). The quality of the assessment determines not only the identification of problems, but also the organization’s ability to effectively eliminate them and increase the maturity of the CMS.

International standards ISO 37301, ISO 37001, COSO ERM, and IIA standards create a methodological framework for such an assessment, forming a unified approach to ensuring transparency, integrity, and accountability in the activities of organizations.

The compliance management system maturity model is a tool that allows you to assess the level of development of a compliance system based on a set of quantitative (KPI) and qualitative indicators. Its main goal is to determine the stage of development of the compliance system, which areas need improvement, and what resources should be involved to move to a higher level.

The model is based on the principles of: ISO 37301:2021 – Compliance Management Systems; ISO 31000:2018 – Risk Management; COSO ERM – Enterprise Risk Management Framework; IIA Standards – Performance and Assurance of Internal Audit.

The main criteria for assessing maturity are: management policy and commitment (existence of a compliance policy, role of management, level of integration into corporate governance); identification and assessment of non-compliance risks (systematic assessment, documentation, risk prioritization); control procedures and internal monitoring (effectiveness of preventive, detective, and corrective measures); training, communication, and integrity culture (scope of training, level of staff involvement, corporate ethics); response and corrective actions (mechanisms for responding to violations, transparency of investigations, reporting); performance evaluation and improvement (use of KPIs, internal audit, self-assessment, improvement measures).

The result of the methodological process is the CMS maturity level (Maturity Model) (Initial / Developing / Established / Advanced / Optimized). ISO 37302 recommends using a five-level maturity scale to assess the stage of development of the system (Table 10.11).

Table 10.11 - Five-level maturity scale in accordance with ISO 37302 requirements

Level	Level Name	System Characteristic	Key Features
Initial	No system or a fragmented system	There is no formalized compliance policy, and the approach is reactive	Cases of violations are resolved on an ad hoc basis

Defined	Foundations are being established	There are individual procedures and responsible persons, but no integrated system	Control measures are inconsistent
Implemented	A formalized system has been established	There is a compliance policy, basic risk analysis procedures, and staff training	Activities are coordinated centrally
Managed	The system operates effectively	KPIs, continuous monitoring, audit, and analytics are used	A culture of integrity is being actively developed
Optimized	The system is integrated into corporate governance	A risk-based approach, digital tools, and regular improvement are used	Compliance is part of strategic management

To quantify the level of maturity, the Compliance Maturity Index (CMI) is used, which is calculated using the following formula:

$$\text{CMI} = \frac{\sum_{i=1}^{n} W_i * S_i}{\sum_{i=1}^{n} W_i}$$

S_i – evaluation of each criterion (1–5),

W_i – weight coefficient (according to the importance of the criterion),

n – number of criteria.

Table 10.12 Maturity assessment ranges in accordance with ISO 37302 requirements

CMI Value	Maturity Level	Interpretation
4.5–5.0	Optimized	High maturity, integration into business processes
3.5–4.4	Managed	The system is effective and control is stable
2.5–3.4	Standardized	A foundation exists, but improvements are needed

1.5–2.4	Basic	Initial steps have been taken, but the system remains inconsistent
1.0–1.4	Initial	There is no effective compliance system

Thus, KPIs serve as the basis for quantitative assessment, while maturity levels serve as the basis for qualitative analysis of the system's development. This approach allows for the creation of a dynamic compliance management system focused on continuous improvement.

Table 10.13 Example of an integrated assessment structure

Criterion	KPI	Weight (wi)	Score (Si)	Weighted Score (wi × Si)
Policy and leadership	Existence of an approved policy, frequency of updates	0.20	4	0.8
Risk management	Conducting compliance risk assessment	0.25	3	0.75
Control mechanisms	Frequency of monitoring, level of violations	0.15	5	0.75
Culture and training	Share of staff covered by training	0.20	4	0.8
Effectiveness assessment	Use of KPIs, reporting, audit	0.20	3	0.6
Integral CMI indicator				**3.7 ("Managed" level)**

Thus, the combination of qualitative and quantitative methods allows building a comprehensive compliance effectiveness assessment system focused on continuous improvement and strategic maturity of the organization.

The integrated model for assessing the maturity of a compliance management system ensures the unity of quantitative (KPI) and qualitative assessment, allows for an objective determination of the level of development of the compliance system, contributes to the formation of an improvement plan, creates a basis for external certification under ISO 37301, and enhances the transparency and accountability of corporate governance.

10.6. Independent assessment and external confirmation of the effectiveness of the compliance system

Independent assessment and external confirmation of the effectiveness of the compliance system involve engaging external experts, auditors, or certification bodies to objectively analyze, verify, and confirm the effectiveness of the compliance management system (CMS).

Such external confirmation ensures the impartiality of the assessment, increases the level of trust on the part of regulators, partners, and society, and is an important condition for the maturity of the compliance system in accordance with the requirements of ISO 37301:2021 and ISO 37302:2025 standards.

External suppliers are legal entities or individuals (consulting companies, law firms, IT providers, certification bodies, training centers, specialized whistleblowing solution providers, etc.) that provide an organization with the expert, technical, or operational services necessary to establish, maintain, monitor, and evaluate a compliance management system (Table 10.14).

Table 10.14 Classification of suppliers and typical profiles

Types of Providers	Services	Profile
Consulting firms (compliance consulting)	Development of policies, gap analysis (comparison with ISO 37301/37302, etc.), CMS implementation, procedure development, risk mapping, CAPA plans	Auditors, compliance officers, legal experts, project managers
Law firms	Legal support, interpretation of legislation, support during regulatory inspections, contract drafting, due diligence	Lawyers specializing in corporate law, competition law, AML, GDPR, and labour law
External audit and external assurance providers	Conducting independent audits, peer reviews, assessment of control effectiveness, preparation of reports for the board	Certified auditors
IT providers (SaaS solutions for compliance)	Systems for incident registration, whistleblowing platforms, case management, KYC/AML systems, risk registers, analytics (data analytics), process mining	Software developers, cloud solution providers, cybersecurity providers

Training and e-learning providers	Courses on compliance, anti-corruption, conflicts of interest, training for management, awareness testing	Trainers, academic partners, LMS content developers
Due diligence and third-party screening providers	Counterparty checks, beneficial ownership verification, sanctions screening, reputation checks	Specialized screening services, OSINT analysts
Certification and standardization bodies	Independent compliance assessments (ISO 37301 certification), recommendations on the implementation of standards	Accredited certification bodies
External investigators and internal investigation specialists	Independent incident investigations, criminal law expertise, digital forensics	Certified specialists

When selecting external suppliers, it is important to evaluate not only the cost of services, but also quality, reputation, competence, and cultural compatibility.

It is recommended to conduct a minimum check of compliance service providers' compliance with the requirements of the compliance management system (CMS), which includes the following steps:

1. Assessment of competence and experience – verification of experience in the relevant industry, completed cases, knowledge of local and international legislation, as well as professional qualifications (CFE, CAMS, CCEP, ISO Auditor, IIA, etc.).

2. Reputation and feedback analysis – studying customer recommendations, case studies, independent reviews, and ratings.

3. Verification of independence and absence of conflicts of interest – confirmation of the absence of connections that could affect objectivity, the existence of confidentiality policies and ethical standards.

4. Agreement on methodology and tools – defining a clear methodology for performing work, standard templates, analytical tools, and checklists.

5. Assessment of technological capabilities – availability of modern IT solutions, analytical dashboards, and integration capabilities with ERP or CRM systems.

6. Verification of legal and regulatory compliance – compliance with GDPR and local data processing legislation, availability of accreditations and licenses.

7. Analysis of financial stability and commercial terms – transparency of pricing policy, flexibility of payment model, availability of SLA.

8. Assessment of interaction culture – ability to work in partnership with internal teams, communication skills, and adaptability.

This approach ensures high-quality, ethical, and secure cooperation with suppliers, minimizes the risks of non-compliance, and increases trust in external experts.

When working with external suppliers, the following risks may arise: risk of conflict of interest (to minimize them by establishing a clear policy, disclosing connections, prohibiting related services); risk of loss of control over data (to minimize them by establishing encryption, data localization, personal data processing agreements (DPA), security audits); risk of poor service quality (minimized by establishing SLAs, phased acceptance, warranty periods, penalties); risk of vendor lock-in (minimized by establishing data export requirements, open standards, backup options); reputational risk (to minimize it by establishing preliminary reputation checks, clauses on compliance with ethical standards); legal risks (liability, regulatory sanctions) (to minimize them by establishing insurance (Professional Indemnity), clear liability provisions).

One of the external providers may be an external audit. An external audit of the compliance management system is an independent, objective, and systematic review conducted by third-party audit organizations or certified auditors to assess the effectiveness of the CMS, verify compliance with standards, legislation, and corporate policies, determine the maturity and effectiveness of compliance measures, and identify risks, gaps, and opportunities for system improvement.

Maximilian Jantz and Stephan Grüninger (2013) in their article “Auditing Compliance Management Systems” “Prüfung von Compliance-Management-Systemen,” noted that the effectiveness of CMS is assessed according to two key criteria: angemessene (adequacy/appropriateness) – the system corresponds to the risks and requirements of the company, and wirksamkeit (effectiveness) – the system actually works and ensures compliance with standards. “Compliance measures are adequate if they are suitable to prevent or significantly impede violations.” “Effectiveness requires that planned measures are implemented and achieve detection and prevention.” They define three levels of CMS verification: conceptual (Konzeptionsprüfung), adequacy (Angemessenheitsprüfung), and effectiveness (Wirksamkeitsprüfung). Maximilian Jantz and Stephan Grüninger emphasize that auditing cannot guarantee absolute effectiveness due to the human factor and the possibility of system fraud. “Even an effective CMS cannot fully prevent violations... management override remains possible.” They stress the importance of combining documentary verification with process tests and selective analysis of evidence of practical implementation of measures. They note the need to integrate compliance into corporate governance, support a culture of integrity, and ensure a balance between internal and external audits.

External auditors provide an objective view of the system’s performance because they are not part of the organization. This allows for the unbiased identification of risks of non-compliance or a formal approach to compliance, avoiding “internal bias” or subjective assessments, and confirming the actual level of effectiveness and maturity of the CMS. Such an external assessment provides transparency and accountability, which strengthens the trust of shareholders and business owners, regulators, business partners, employees, and the public.

10.7. Continuous improvement of the compliance management system

Continuous improvement of compliance management is a continuous process of systematic analysis, updating, and optimization of policies, procedures, and control mechanisms that ensure compliance with legislative, regulatory, ethical, and internal organizational requirements.

According to the international standard ISO 37301:2021, continuous improvement is one of the key principles of a compliance management system and is based on the PDCA (Plan – Do – Check – Act) cycle. This approach involves the system responding dynamically to changes in the internal environment, legislation, and risks associated with the organization's activities (Figure 10.5).

The goal of continuous improvement is to ensure the maturity and effectiveness of the compliance management system, increase trust on the part of regulators, partners, and society, and promote a culture of integrity within the organization.

PLAN	DO	CHECK	ACT
–defines compliance objectives in line with strategic priorities and risks; –analyzes legislative changes, regulatory requirements, and the results of previous audits; –updates the compliance risk map; –develops an action plan to improve the effectiveness of the compliance management system.	–new policies, procedures, and standards of conduct are being implemented; –staff training, workshops, and explanatory events are being held; –technical solutions (automated controls, risk monitoring systems) are being applied.	–monitoring the effectiveness of the compliance management system through audits, internal checks, analysis of incidents and complaints; –evaluating key performance indicators (KPIs) - number of violations detected, timeliness of response, frequency of policy updates, etc.; –the results of the analysis are documented in compliance service or internal audit reports.	–corrective and preventive actions are developed based on the results of audits. –internal documents, standards of conduct, and regulations are updated. –feedback from employees and stakeholders is implemented. –management conducts a Management Review to assess the effectiveness of the compliance system and make strategic decisions for improvement.

Figure 10.5 - PDCA continuous improvement cycle

The implementation of PDCA in compliance covers six interrelated areas: risk management, digitization of controls, development of a culture of integrity, assessment and internal audit, CAPA, and interaction with stakeholders. Areas of continuous improvement in the compliance management system include:

> first, analysis and monitoring of compliance risks, which involves regularly updating the risk map, using a risk-based approach to planning controls, and integrating compliance risks into the overall risk management system;

- secondly, digitization of compliance processes, which involves the use of analytics, artificial intelligence, and automated monitoring systems, the creation of electronic registers of violations, control reports, and risk indicators;
- thirdly, the development of a culture of integrity, which involves staff training, the formation of ethical standards of conduct, the introduction of effective whistleblowing mechanisms, and the promotion of ethical leadership by top management;
- fourth, assessing the effectiveness of the compliance management system and internal audit, which includes conducting regular internal and external compliance audits, independent assessment of the maturity of the compliance management system according to international models (e.g., maturity models), and engaging external consultants for expert assessment of compliance practices;
- fifth, corrective and preventive actions (CAPA), which include documenting all identified non-conformities, eliminating their causes, not just their consequences, and preventing recurrence of violations through changes in procedures;
- sixth, interaction with stakeholders, which involves openness to regulators, partners, shareholders, disclosure of compliance reports, and exchange of experience and benchmarking (comparison with best practices in the industry).

Continuous improvement of compliance management is not a one-time action, but a cyclical strategic process that ensures the evolution of the compliance system in line with changes in legislation, market conditions, and public expectations. It is based on the principles of transparency, accountability, and continuous learning and aims to move from formal control to active, risk-based integrity management. Such a system becomes the foundation for sustainable corporate development, improves corporate governance, and ensures the long-term reputational stability of the organization in a global environment.

Practical Exercises

Exercise 1 – "Paper Compliance" vs Real Outcomes

Situation: The company has a complete set of compliance policies, but over the year the number of incidents has not decreased, and employees complain that trainings are purely formal.
Tasks:

- Identify which principles of effectiveness evaluation are violated (system approach, outcome-based evaluation, evidence-based approach, continual improvement).
- Propose 3 sources of evidence that distinguish "having documents" from "real behavioural impact".
- Formulate one conclusion for management review using PDCA logic.
  Note: Refer to the idea "evaluate the system, not isolated measures" (Soltes) and ISO 37302 (evidence/outcomes).

Exercise 2 – Building an "Evaluation Tools Map"

Situation: A new compliance officer asks HR/Internal Audit/Legal to define what exactly will be used to measure CMS effectiveness.
Tasks:

- Categorize evaluation tools into five groups: document review, interviews/ focus groups, surveys, control testing, data analytics/BI.
- For each group, propose two examples of artefacts/data (what exactly will be collected).
- Indicate which tools are best for "culture and behaviour" and which are best for "processes and controls".
  Note: Apply the principle of proportionality (ISO 37302).

Exercise 3 – KPI / KRI / PI: What's What?

Situation: The Board requests 10 "compliance indicators" but confuses KPIs, KRIs, and PIs.
Tasks:

- Provide three indicators for each type: KPI, KRI, PI.
- For two indicators, propose a formula, data source, and frequency.
- Explain how these indicators work within the PDCA cycle (Plan–Do–Check–Act).
  Note: Indicators must be SMART and linked to risks.

Exercise 4 – Assessing CMS Maturity (Maturity Model)

Situation: The company is preparing for ISO 37301 certification and wants to determine its maturity level using an ISO 37302-style approach.
Tasks:

- Propose five maturity levels (Initial → Optimized) with short characteristics for each.
- Create a mini-matrix with 6 criteria (leadership, risks, policies, training, reporting channels, monitoring) and a 1–5 scale.
- Calculate a maturity index (CMI) using a weighted approach (specify weights).
  Note: Show a system approach and continual improvement.

Exercise 5 – "Power Few": Risk Concentration in Key Roles

Situation: Incidents occur most often in three units and among a small group of "key individuals".
Tasks:

- Identify which roles/processes are the "power few" in your industry

(procurement, sales, M&A, licensing, etc.).

> Propose two targeted evaluation tools for these groups (not generic “training for all”).

> Formulate two KRIs that signal “extreme” risks.
Note: Use Todd Haugh’s behavioural focus and ISO 37301/37302 risk-based thinking.

Exercise 6 – Ethical Culture as “Control #1”

Situation: The system works formally, but a survey shows low trust and fear of reporting misconduct.
Tasks:

> Draft five questions for an “Ethics Culture Survey” (trust, fairness, leadership example, willingness to speak up, no retaliation).

> Propose an Ethics Culture Index (how to score: scale, average score, thresholds).

> Indicate two management decisions that should follow from the index results.
Note: Avoid formality; follow logic: “culture matters more than policies”.

Exercise 7 – Effectiveness of Reporting Channels and Whistleblower Protection

Situation: A hotline exists, but there are almost no reports.
Tasks:

> Identify three possible reasons (lack of trust, confidentiality concerns, fear of consequences, unclear procedures).

> Propose two indicators of channel effectiveness (not only “number of reports”).

> Explain how to verify alignment with Ukrainian whistleblower rules (Law “On Prevention of Corruption”, Art. 53–53⁴) regarding protection/confidentiality/feedback.
Note: Evaluate both process (PI) and trust/culture (behavioural metrics).

Exercise 8 – Data Analytics for Evaluating CMS Effectiveness

Situation: The company has a BI dashboard (ERP/HR/Procurement). A “compliance analytics pack” is needed.
Tasks:

> Identify two risks that can be detected via analytics (abnormal payments, split procurements, conflicts of interest, abuse of authority).

> Propose three red-flag rules/signals and who reviews them.

> Describe ethical safeguards for using employee data (data minimization, access control, logging, purpose limitation).

Note: Align with labour law requirements and personal data protection norms.

Exercise 9 – Monetising Compliance: Value & ROI

Situation: The CFO asks: “How much does compliance cost and what is the benefit?”
Tasks:

- Classify costs into one-off and ongoing (people, IT, training, audits).
- Propose three measurable benefits (avoided fines/losses, fewer incidents, lower cost of capital/tender advantages—if relevant).
- Provide a simple compliance ROI formula and an example calculation using illustrative numbers.
  Note: Follow Westhausen’s approach (activity/result/behaviour returns).

Exercise 10 – Annual Effectiveness Evaluation Plan

Situation: The organization must approve an annual “Check” plan in PDCA for the CMS: what, when, and by whom it is evaluated.
Tasks:

- Develop an annual evaluation calendar: self-assessment, internal audit, culture survey, KPI/KRI review, management review, CAPA follow-up.
- Define RACI (who is responsible: Compliance/HR/Legal/Internal Audit/IT/Top management).
- Add five key deliverables (effectiveness report, updated risk map, CAPA plan, KPI/KRI dashboard, management report).
  Note: The plan must be proportionate to risks and demonstrate continual improvement.

Target Questions

1. What is the difference between monitoring, measurement, analysis, and evaluation in a compliance management system?
2. How does the PDCA cycle (Plan–Do–Check–Act) support continuous improvement of compliance?
3. Why is it important to assess compliance as a system, not as separate activities?
4. What is the difference between KPI, KRI, and PI?
5. Which data sources can be used to track compliance indicators?
6. Name four key principles for evaluating compliance effectiveness (e.g., objective, risk-based, evidence-based, outcome-focused).
7. What are the main steps of an effectiveness evaluation?

8. What is a scoring scale (e.g., 1–5), and why is it useful for comparing results over time?
9. What is a maturity model for compliance, and what does a higher level usually mean?
10. Why should a company pay special attention to high-risk roles or departments when evaluating compliance?
11. What are three simple ways to measure ethical culture and trust inside an organization?
12. How can an organization show the value of compliance (costs vs benefits)?
13. What methods are used to evaluate effectiveness?
14. How does a risk-based approach influence the effectiveness of a compliance management system?
15. What does continual improvement of a compliance management system mean under ISO 37302?
16. What sources of information can be used during an evaluation (reports, surveys, audits, observations)?
17. What are the most common mistakes made when assessing effectiveness?
18. How can an effectiveness evaluation help improve a company's reputation?

List of references for independent study

1. OECD. (n.d.). Anti-corruption and integrity. https://www.oecd.org/corruption-integrity/.
2. Coglianese, C., & Nash, J. (2021). Compliance management systems: Do they make a difference? In D. D. Sokol & B. van Rooij (Eds.), The Cambridge handbook of compliance. Cambridge University Press. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3598264.
3. Gammisch, M., & Balina, S. (2014). The effectiveness of compliance management systems: An experimental approach. In Proceedings of the 19th International Scientific Conference Economics and Management 2014 (ICEM 2014), Riga, Latvia. https://www.researchgate.net/publication/275544916_The_Effectiveness_of_Compliance_Management_Systems_-_An_Experimental_Approach.
4. Westhausen, H.-U. (2021). About the calculation of the compliance value and its practical relevance. Ekonomika, 100(2), 171–189. https://www.econstor.eu/bitstream/10419/323103/1/1795127821.pdf
5. Lam, H.-P., & Hashmi, M. (2022). A comparative study of compliance management frameworks: PENELOPE vs. PCL. Knowledge, 2, 618–651. https://www.mdpi.com/2673-9585/2/4/36

6. International Organization for Standardization. (2025). ISO 37302:2025 compliance management systems—Guidelines for performance evaluation. ISO. https://cdn.standards.iteh.ai/samples/75081/7804b1c42db74019b845bca7c74acc44/ISO-FDIS-37302.pdf

7. International Organization for Standardization. (2025). ISO 37302:2025 compliance management systems—Guidelines for the evaluation of effectiveness. ISO. https://cdn.standards.iteh.ai/samples/75081/7804b1c42db74019b845bca7c74acc44/ISO-FDIS-37302.pdf

8. International Organization for Standardization. (2021). ISO 37301:2021 compliance management systems—Requirements with guidance for use. ISO. https://cdn.standards.iteh.ai/samples/75080/98db41625e0445a193a12f005dd5f30b/ISO-37301-2021.pdf.

9. International Organization for Standardization. (2016). ISO 37001:2016 anti-bribery management systems—Requirements with guidance for use. ISO. https://www.wfeo.org/wp-content/uploads/stc-anticorruption/ISO37001_Preview.pdf.

10. International Organization for Standardization. (2018). ISO 31000:2018 risk management-Guidelines. ISO. https://cdn.standards.iteh.ai/samples/65694/60673072317a4b96bd36efb910b68926/ISO-31000-2018.pdf.

11. nternational Organization for Standardization. (2014). ISO 19600:2014 compliance management systems—Guidelines. ISO. https://cdn.standards.iteh.ai/samples/62342/70f1bb105d814e8894e17f65a773e7f0/ISO-19600-2014.pdf

12. Zielinski, J. (n.d.). The effectiveness of your compliance program. New Perspectives, Association of Healthcare Internal Auditors, 40(3). https://www.dinsmore.com/content/uploads/2021/06/40-3-The-Effectiveness-of-Your-Compliance-Program-by-Zielinski.pdf.

13. Remmerbach, K.-U., & Krumme, R. (2020). The effectiveness of compliance management systems. https://d-nb.info/1324097701/34.

14. Groenewald, L., & Dondé, G. (2017). Ethics and compliance handbook. The Ethics Institute & Institute of Business Ethics. https://www.tei.org.za/wp-content/uploads/2020/04/Ethics-and-Compliance-Handbook.pdf.

15. Jin, L., He, C., Wang, X., Wang, M., & Zhang, L. (2020). The effectiveness evaluation of system construction for compliance management in the electricity market. IOP Conference Series: Earth and Environmental Science, 647, 012024. https://doi.org/10.1088/1755-1315/647/1/012024

16. González Calvet, M., Vazquez, K., Gonzalez, B., Ferrante, C., & Majercin, C. (2024). Building effective internal communication channels. In The guide to corporate compliance. https://www.ropesgray.com/-/media/files/articles/2024/06/061524_latin_lawyer_article.pdf.

17. Jantz, M., & Grüninger, S. (2013). Prüfung von compliance-management-systemen (KICG Forschungspapier Nr. 7). HTWG Konstanz. https://www.htwg-konstanz.de/fileadmin/pub/ou/kicg/KICG-Forschungspapiere/KICG_Forschungspapier_7_Pruefung_von_Compliance_Management_Systemen.pdf/.

18. Mekuria, M. B. (2016). Perceptions on an effective compliance management system (Master's thesis). https://www.diva-portal.org/smash/get/diva2:956990/FULLTEXT01.pdf.

19. Organisation for Economic Co-operation and Development. (2023). OECD guidelines for multinational enterprises on responsible business conduct. OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/06/oecd-guidelines-for-multinational-enterprises-on-responsible-business-conduct_a0b499

20. Organisation for Economic Co-operation and Development. (n.d.). OECD convention on combating bribery of foreign public officials in international business transactions. https://www.oecd.org/corruption-integrity/explore/oecd-standards/anti-bribery-convention/

21. Organisation for Economic Co-operation and Development. (n.d.). Recommendation of the OECD public integrity council. https://www.oecd.org/corruptionintegrity/explore/oecd-standards/integrity-recommendation/

22. Organisation for Economic Co-operation and Development. (n.d.). Recommendation on addressing corruption risks in development cooperation agencies. https://www.oecd.org/corruption-integrity/explore/oecd-standards/managing-risk-corruption-development/

23. Transparency International. (n.d.). Publications. https://www.transparency.org/en/publications

24. Müller, R., Bühr, D. L., & Maurhofer, R. (n.d.). Sicherstellung der compliance auf strategischer Führungsebene. https://www.alexandria.unisg.ch/server/api/core/bitstreams/7e58d4c5-c8b7-4668-aa8d-30e08e0090a9/content

25. Soltes, E. F. (2018). Evaluating the effectiveness of corporate compliance programs: Establishing a model for prosecutors, courts, and firms. NYU Journal of Law & Business, 14(3), 965–1011. https://www.scribd.com/document/412530256/Eugene-Soltes-2018

26. Internal Audit Unit of FSA Cambodia. (n.d.). The excellence of compliance management. https://iauoffsa.gov.kh/wp-content/uploads/2023/12/5-The_excellence_of_compliance_management.pdf

27. Transparency International Ukraine. (n.d.). Research. https://ti-ukraine.org/research/

28. Transparency International. (2023). Global corruption report 2023. Transparency International Secretariat. https://transparencia.org.es/wp-content/uploads/Report_CPI2023_English.pdf

29. Haugh, T. (2018). The power few of corporate compliance. Georgia Law Review, 53(1), Article 3. https://digitalcommons.law.uga.edu/glr/vol53/iss1/3

30. United Nations Office on Drugs and Crime. (n.d.). Corruption and Economic Crime Branch: Guardian of the United Nations Convention against Corruption. https://www.unodc.org/corruption/index.html

31. United Nations Office on Drugs and Crime. (n.d.). United Nations Convention against Corruption. https://www.unodc.org/corruption/en/uncac/learn-about-uncac.html

32. U.S. Department of Justice. (2020). Evaluation of corporate compliance programs. U.S. Department of Justice. https://www.worldcomplianceassociation.com/componentes/editor/ckfinder/userfiles/files/evaluation-of-corporate-compliance-programs-june-2020-revision.pdf

33. Volkov, M. (2018). Ethics and the definition of successful companies. Corporate Compliance Insights. https://www.corporatecomplianceinsights.com/wp-content/uploads/2018/10/Its_The-Culture_Stupid_By_M_Volkov.pdf

34. World Bank Group. (n.d.). World Bank official website. https://www.worldbank.org/

35. Okuniev, O., Shenk, O., Varenyk, M., Derkach, S., Lutsiuk, S., Lahodiienko, O., & Verkhniatskyi, P. (2023). Anti-corruption compliance: A guide for training persons responsible for implementing anti-corruption programs (2nd ed.). https://cgpa.com.ua/wp-content/uploads/2023/04/Komplaens_2023_04-2023_web.pdf

36. Hura, V. (2023). Compliance system as a way to combat corruption. Economy and Society, 52. https://economyandsociety.in.ua/index.php/journal/article/view/2604

37. Dymenko, R. A. (2019). Formation of a structural-logical model for implementing compliance policy in the telecommunications industry. Market Economy: Modern Management Theory and Practice, 18(3(43)), 200–216. http://rinek.onu.edu.ua/article/view/183683

38. Verkhovna Rada of Ukraine. (2014). On prevention of corruption (Law No. 1700-VII). https://zakon.rada.gov.ua/laws/show/1700-18

39. Verkhovna Rada of Ukraine. (1996). On accounting and financial reporting in Ukraine (Law No. 996-XIV). https://zakon.rada.gov.ua/laws/show/996-14

40. Verkhovna Rada of Ukraine. (1993). On the basic principles of public financial control in Ukraine (Law No. 2939-VI). https://zakon.rada.gov.ua/laws/show/2939-12

41. Organisation for Economic Co-operation and Development. (n.d.). OECD integrity and anti-corruption review of Ukraine. https://www.oecd.org/uk/publications/5f7daca7-uk/full-report/business-integrity-policy-and-awareness-raising_25d6c18e.html

42. Omelchuk, Y., & Kochuma, I. (2018). Basic principles of organizing an effective compliance control system and problems of their implementation in Ukrainian banks. Financial Space, 1(29). http://fp.lnu.edu.ua/index.php/fp/article/view/571

43. Pylypenko, H. S., & Krasnova, I. V. (2025). Compliance management in the banking sector of Ukraine: Theoretical and practical aspects of implementation and improvement. Efficient Economy, 2. https://www.nayka.com.ua/index.php/ee/article/view/5771

44. Verkhovna Rada of Ukraine. (2010). Tax Code of Ukraine (Law No. 2755-VI). https://zakon.rada.gov.ua/laws/show/2755-17.

45. Sahaidak, M. P., & Maryniuk, I. O. (2024). Study of the theoretical foundations of the formation of compliance management systems of organizations. Scientific Notes of Vadym Hetman Kyiv National Economic University, 37, 108–120. https://ir.kneu.edu.ua/items/c08dc941-ec24-4af4-ab06-691fe2113797.

46. Seleznova, H. O., & Ippolitova, I. Ya. (2020). Evaluation of the effectiveness of enterprise management systems. Efficient Economy, 3. http://www.economy.nayka.com.ua/?op=1&z=7711.

47. Khavanov, A. V. (2025). Development and implementation of compliance indicators for assessing the maturity of enterprise economic security systems. Economic Space, 201. https://economic-prostir.com.ua/wp-content/uploads/2025/06/201-230-233-havanov.pdf.

48. Shalimova N. (2024). Internal Audit and Compliance management: Interconnection and Perspective. *«Sustainable Transport Systems and Maritime Logistics» ISTSML – 2024 : Book of proceedings of* VIII International Scientific Conference Dedicated to The International Day of The Seafarers (pp. 14-21), Batumi, BNTU. https://conference.bntu.nier.ge/images/Proccedings_A5%202024_FINAL.pdf

49. Shalimova N., & Fomenko A. (2024). Interconnection Between Compliance Management System and Internal Audit. *Development of Accounting, Auditing and Taxation under the Conditions of Innovative Transformation of Socio-Economic Systems:* Proceedings of the 12th International Scientific and Practical Conference, December 5, 2024 (pp. 376-378). Kropyvnytskyi: CUNTU. https://audit.kntu.kr.ua/file/content/13890/2024_tez[1].pdf

50. Shalimova, N., & Kozachenko, Ya. (2024). Transformation of approaches to the implementation of internal audit in modern business structures: assurance, compliance, and forensic services. *Central Ukrainian Scientific Bulletin. Economic Sciences*.12(45), 307-318. https://doi.org/10.32515/2663-1636.2024.12(45).307-318 [in Ukrainian]

51. Shvydka, T., & Khaletska, K. (2020). Compliance control in the system of corporate governance of business entities. Commercial Law and Procedure, 12, 85–90. http://pgp-journal.kiev.ua/archive/2020/12/15.pdf.

Assignments for Self-Study

1. *Essay: From "Paper Compliance" to Real Outcomes (2 pages).* Explain why assessing a compliance management system must be outcome-focused and evidence-based rather than limited to checking documents. Clarify the difference between monitoring, measurement, analysis, and evaluation, and show how PDCA supports continual improvement. Provide 3 examples of "paper evidence" vs 3 examples of real behavioural evidence.

2. *Mini-Case Study: Annual Compliance Effectiveness Evaluation Plan (3–4 pages).* Assume an organization needs quarterly proof that its compliance management system works. Design a 12-month ISO 37302-style evaluation plan: define scope

and criteria, choose evaluation methods, identify information sources, create an evaluation calendar (self-assessment, internal audit, surveys, KPI/KRI/PI analytics, management review), and list key deliverables (effectiveness report, risk map update, CAPA plan, dashboard).

3. *Comparative Table: KPI vs KRI vs PI in Compliance (1–2 pages).* Create a table that compares KPIs, KRIs, and PIs in simple terms. Provide at least 5 indicators of each type for a chosen sector (e.g., energy, logistics, manufacturing, public sector) and specify for each: formula/method, data source, frequency, owner, and threshold/target. Conclude with short recommendations on building a balanced indicator set.

4. *Practical Task: Compliance Maturity Model and Compliance Maturity Model Calculation (2 pages).* Develop a simple 5-level maturity model (Initial → Optimized) and assess a real or hypothetical organization using 6 criteria (leadership, risk management, policies/procedures, training, reporting channels, monitoring/audit). Apply a 1–5 scoring scale and weighted scoring, calculate a Compliance Maturity Index (CMI), and propose 3 priority improvement actions (CAPA).

5. *Applied Analysis: Compliance Value and ROI (2 pages).* Prepare a short note for management explaining the value of compliance. Separate one-off vs ongoing costs, list at least 5 benefits (including at least 2 that can be monetised), propose a simple ROI/value formula, and illustrate it with an example using assumed numbers. Distinguish leading vs lagging indicators to support the argument.

6. *Policy Brief: External Evaluation and Provider Selection (1–2 pages).* Describe when external/independent evaluation is needed (e.g., certification readiness, high-risk changes, repeated incidents) and when internal methods are sufficient. Propose clear criteria for selecting external providers (competence, independence, methodology, data security, KPIs). Identify key outsourcing risks (conflict of interest, data loss, vendor lock-in) and how to mitigate them.

Chapter 11: Compliance Management for ESG Goals, Corporate Sustainability and Social Impact

Learning Outcomes

By the end of this chapter, readers will be able to:

> Explain the role of compliance management in ensuring ESG (environmental, social, and governance) performance and corporate sustainability.

> Analyse EU and Ukrainian regulatory frameworks and their application to ESG compliance.

> Design compliance strategies that enhance corporate social impact.

Key Words: Compliance, ESG, corporate sustainability, social impact, governance, accountability, regulations, stakeholder engagement.

Main Definitions

Compliance Management **-** A structured system of policies, procedures, and monitoring mechanisms designed to ensure conformity with legal, regulatory, and ethical obligations, reducing the risk of misconduct and fostering organizational integrity (Kaptein, 2011).

ESG Goals - Organizational objectives focusing on environmental protection, social responsibility, and governance effectiveness, forming a framework for sustainable value creation and stakeholder accountability (Friede, Busch, & Bassen, 2015).

Corporate Sustainability - An integrated approach combining economic performance with long-term environmental stewardship and social equity, ensuring resilience in a rapidly changing global context (Dyllick & Muff, 2016).

Corporate Social Responsibility (CSR) - A concept in which companies voluntarily integrate social and environmental concerns into business operations and stakeholder interactions, laying the foundation for ESG frameworks (Carroll, 1991).

Governance - The set of systems, processes, and structures by which companies are directed and controlled, ensuring accountability, transparency, and compliance with legal and ethical standards (OECD, 2015).

Social Impact - The positive or negative consequences of corporate activities on stakeholders, communities, and society, often measured through employment, health, education, and equity outcomes (Maas & Liket, 2011).

Stakeholder Engagement - The process of identifying, involving, and responding to groups affected by corporate decisions, ensuring that compliance and ESG efforts align with diverse expectations (Freeman, 1984).

Greenwashing - A deceptive practice where organizations exaggerate or misrepresent

their ESG or sustainability efforts, undermining compliance credibility and stakeholder trust (Delmas & Burbano, 2011).

Sustainability Reporting - The structured disclosure of environmental, social, and governance performance, typically aligned with frameworks such as GRI, CSRD, or ISO standards, to demonstrate accountability (KPMG, 2020).

Risk Management in ESG Compliance - The systematic process of identifying, assessing, and mitigating ESG-related risks (e.g., climate change, human rights, governance failures) that can affect corporate resilience (Eccles & Klimenko, 2019).

Standards, Laws, and Regulations

Compliance management for ESG, corporate sustainability, and social impact is anchored in a complex web of legal requirements, voluntary standards, and international frameworks. These instruments provide the guidelines, reporting obligations, and enforcement mechanisms that ensure organizations act transparently and responsibly.

1. European Union

Corporate Sustainability Reporting Directive (CSRD, 2022). The CSRD significantly expands the scope of sustainability reporting in the EU. While its predecessor, the NFRD, applied to around 11,000 companies, the CSRD covers more than 50,000 firms across the Union. It requires detailed disclosure on environmental, social, and governance (ESG) risks, policies, and outcomes, with mandatory auditing of sustainability reports (European Commission, 2022). For compliance management, this directive means that sustainability reporting is no longer voluntary or superficial but a legally enforceable corporate obligation.

EU Taxonomy for Sustainable Activities (2020). This regulation establishes a classification system for environmentally sustainable activities, allowing investors and regulators to determine whether an economic activity is “green.” For compliance purposes, companies must align their business activities and investments with the taxonomy to access sustainable financing and meet EU disclosure rules (EU Regulation 2020/852). It is a cornerstone of the European Green Deal.

Non-Financial Reporting Directive (NFRD, 2014). The NFRD was the EU’s first legislative attempt to introduce sustainability disclosure obligations. It required large public-interest entities (over 500 employees) to disclose information on environmental matters, social and employee-related aspects, human rights, and anti-corruption policies. While limited in scope, it laid the groundwork for the CSRD. Compliance managers must understand the NFRD both as a historical benchmark and as the legal framework still relevant for smaller firms until CSRD is fully implemented.

2. Ukraine

Law on Accounting and Financial Reporting (amended, 2017). This law brought Ukraine closer to EU financial transparency standards. It requires large and public-interest companies to prepare financial statements according to International Financial Reporting Standards (IFRS). Although it focuses primarily on financial compliance, the law created the infrastructure for integrating non-financial (ESG) reporting into Ukrainian

corporate practice (Ministry of Finance of Ukraine, 2017).

National Strategy "Ukraine–2030." Ukraine's long-term development strategy emphasizes the green energy transition, resource efficiency, and responsible governance. While not a binding law, it provides a policy roadmap for sustainable economic growth. For compliance management, it signals where Ukrainian companies must align their strategies to remain competitive and consistent with European integration priorities.

Voluntary ESG Adoption by Large Companies. Ukrainian corporations such as Naftogaz and DTEK have voluntarily implemented ESG reporting frameworks (e.g., GRI, SASB). This practice not only enhances transparency but also improves access to international capital markets, since investors increasingly demand ESG-aligned disclosures. In Ukraine, voluntary compliance often serves as a market-driven substitute for binding legislation.

List of subchapters

11.1 International Frameworks

11.2 Theoretical Foundations of Compliance Management for ESG

11.3 Scholars and Theoretical Approaches

11.4 EU and Ukrainian Examples and Cases

11.5 Case in Point Boxes

11.6 Practical Exercises

11.7 Target Questions

11.8 References for Self-Study

11.9 Assignments for Self-Study

11.1. International Frameworks

In an increasingly globalized economy, businesses operate across multiple jurisdictions, cultures, and regulatory environments. As a result, compliance is no longer limited to national laws and regulations; it also involves aligning with internationally recognized standards and frameworks that promote responsible, ethical, and sustainable business conduct. These international frameworks help organizations manage risks, enhance transparency, strengthen stakeholder trust, and demonstrate accountability beyond minimum legal requirements. Although many of these frameworks are voluntary rather than legally binding, they play a critical role in shaping corporate governance, sustainability strategies, and compliance programs. They provide structured guidance on issues such as human rights, environmental protection, anti-corruption, labour standards, and social responsibility. For compliance officers, understanding and integrating these frameworks into internal policies and reporting systems is essential

for ensuring consistency across borders and meeting the expectations of regulators, investors, and society at large.

The following section outlines key international frameworks that influence modern compliance and corporate responsibility practices.

United Nations Sustainable Development Goals (SDGs, 2015). The SDGs provide a global blueprint for sustainable development across 17 goals, including climate action, gender equality, and responsible consumption. For companies, compliance involves aligning corporate strategies and reporting practices with SDG indicators, even though the framework itself is not legally binding.

OECD Guidelines for Multinational Enterprises (2011). These guidelines provide voluntary principles for responsible business conduct in areas such as human rights, labour, environment, and anti-corruption. For compliance officers, the OECD framework is particularly useful in multinational settings, where cross-border regulatory consistency is needed.

ISO 26000:2010 Guidance on Social Responsibility. This international standard provides guidance (not requirements) for organizations on how to operate in a socially responsible manner. While it is not certifiable like ISO 9001, ISO 26000 is a widely used benchmark for compliance programs, helping companies design policies on stakeholder engagement, fair labour practices, and environmental protection.

A comparison of key documents and recommendations in the field of ESG is presented in Table 11.1.

Table 11.1 - Comparison of ESG-Related Standards, Laws, and Regulations

Framework / Law	Region	Legal Status	Scope of Application	Compliance Impact
CSRD (2022)	EU	Binding Directive	~50,000 EU companies (large & listed SMEs)	Mandatory sustainability reporting; external audit required
EU Taxonomy (2020)	EU	Binding Regulation	Companies & financial institutions	Defines “green” activities; impacts financing and disclosure
NFRD (2014)	EU	Binding Directive (superseded by CSRD)	Large public-interest entities (500+ employees)	First mandatory ESG disclosure law; foundation for CSRD
Law on Accounting & Financial Reporting (2017)	Ukraine	Binding Law	Public-interest & large companies	Aligns with IFRS; basis for integrating ESG disclosure

National Strategy "Ukraine–2030"	Ukraine	Policy Framework (non-binding)	National development priorities	Guides ESG adoption in line with EU integration
Voluntary ESG Reports (Naftogaz, DTEK, etc.)	Ukraine	Voluntary	Large listed companies	Builds investor trust; bridges regulatory gaps
UN SDGs (2015)	International	Voluntary	All UN member states & companies	Provides global sustainability goals; used for alignment
OECD Guidelines (2011)	International	Voluntary	Multinational enterprises	Encourages responsible business conduct; cross-border relevance
ISO 26000 (2010)	International	Voluntary Standard (non-certifiable)	All organizations	Provides guidance for CSR & ESG practices

Together, these laws and frameworks create a multi-layered compliance environment:

> In the EU, compliance is primarily legal and mandatory (CSRD, Taxonomy, NFRD).

> In Ukraine, compliance is evolving, combining legal reforms with voluntary adoption of ESG practices.

> At the international level, compliance relies on widely recognized voluntary standards that guide companies toward responsible and transparent practices.

> The visual flow diagram showing the layers of ESG compliance frameworks:

> International frameworks (UN SDGs, OECD, ISO 26000) provide global guidance.

> EU regulations (CSRD, EU Taxonomy, NFRD) translate these into binding laws for member states.

> Ukraine regulations adapt and align with EU rules, combining binding financial laws with voluntary ESG adoption.

For compliance managers, the challenge is to integrate these instruments into a single coherent system, ensuring that legal obligations, voluntary commitments, and international best practices are aligned with corporate strategy.

11.2. Theoretical Foundations of Compliance Management for ESG

Compliance management forms the backbone of modern ESG strategies because it transforms broad principles of sustainability into measurable, enforceable, and accountable practices. Without compliance, ESG risks becoming a matter of public relations or rhetorical commitments rather than genuine corporate transformation. Compliance ensures that ESG is integrated into business processes, reporting mechanisms, and governance systems, creating a framework for organizations to align their operations with sustainability goals.

The foundations of ESG compliance can be traced back to Corporate Social Responsibility (CSR) theories. One of the most influential models is Carroll's CSR Pyramid (1991), which highlights four layers of corporate responsibility:

1. Economic responsibility – to be profitable and efficient.
2. Legal responsibility – to obey the law.
3. Ethical responsibility – to go beyond the law and act fairly.
4. Philanthropic responsibility – to contribute to society's well-being.

From a compliance perspective, the second layer—legal responsibility—is crucial. Compliance ensures that companies respect environmental laws, labour standards, anti-corruption measures, and financial reporting requirements. However, Carroll's pyramid also demonstrates that compliance alone is not enough. For ESG to be meaningful, organizations must extend beyond minimal legal adherence into ethical and philanthropic dimensions. For instance, a company may comply with minimum carbon emissions regulations, but true ESG commitment involves actively reducing emissions in line with global climate goals.

Triple Bottom Line and ESG Accountability

Elkington's (1997) Triple Bottom Line further advances the theoretical foundation by proposing that businesses should not only measure financial profit (the traditional "bottom line"), but also their performance in terms of people (social impact) and planet (environmental stewardship). This idea laid the groundwork for modern ESG reporting, where compliance requires companies to disclose both financial and non-financial information.

The significance of the Triple Bottom Line in compliance management is twofold:

It broadens the scope of compliance from purely financial/legal aspects to social and environmental concerns.

It embeds accountability into sustainability. If companies are required to publish ESG reports audited under regulations like the EU's CSRD, then sustainability shifts from an optional initiative to a regulated business practice.

Creating Shared Value and Competitive Advantage

Another key theoretical contribution is the Creating Shared Value (CSV) framework developed by Porter and Kramer (2011). They argue that businesses can simultane-

ously create economic value and generate social progress. Compliance plays a vital role in CSV: by ensuring adherence to environmental and labour laws, companies can avoid reputational risks while building trust with stakeholders. Moreover, compliance can generate competitive advantage. For example, firms that align with the EU Taxonomy on sustainable activities gain preferential access to sustainable finance and investment opportunities.

Stakeholder Theory and Governance

Freeman's Stakeholder Theory (1984) underlines the necessity of balancing the interests of multiple stakeholders — customers, employees, regulators, communities, and shareholders. Compliance serves as the institutional mechanism that ensures these interests are respected. For example, labour law compliance protects workers' rights, environmental regulation compliance safeguards community health, and financial compliance ensures shareholder trust.

Governance, the "G" in ESG, is directly tied to compliance theory. According to OECD (2015), corporate governance requires structures of accountability, transparency, and control. A robust compliance system ensures that governance mechanisms function effectively, reducing corruption risks and fostering ethical corporate culture.

Compliance in Transitional Economies

In transitional economies such as Ukraine, compliance takes on a special significance. Regulatory frameworks are often in flux, with governments adopting reforms to align with international and EU standards. This creates both opportunities and challenges:

Opportunities: Ukrainian firms that adopt compliance early gain first-mover advantages by accessing EU markets and ESG-conscious investors. For example, voluntary ESG reporting by companies like Naftogaz demonstrates credibility in global markets.

Challenges: Compliance systems are costly to implement, and many SMEs lack the resources to meet EU-aligned standards. Moreover, institutional weaknesses (e.g., corruption, inconsistent enforcement) undermine confidence in compliance mechanisms (Prokopenko, 2020).

Thus, compliance in Ukraine is not just about obeying rules but about transforming corporate culture to meet EU integration goals.

Compliance as Risk Management

Finally, compliance management is integral to risk management in ESG. Eccles and Klimenko (2019) highlight the "investor revolution," where global investors demand companies disclose climate risks, diversity practices, and governance transparency. Failure to comply creates reputational, legal, financial, and operational risks. In contrast, effective compliance systems act as risk mitigation tools, shielding organizations from fines, scandals, and market exclusion.

The theoretical foundations of compliance management demonstrate that it is not merely a legal obligation, but a strategic and governance imperative. Carroll's CSR Pyramid, Elkington's Triple Bottom Line, Porter and Kramer's Shared Value, and Freeman's Stakeholder Theory collectively emphasize that compliance ensures ESG goals are actionable, measurable, and credible. In transitional economies such as Ukraine,

compliance is both a path to EU integration and a means of building resilience in global markets.

11.3. Scholars and Theoretical Approaches

A variety of scholars have shaped the way businesses, regulators, and academics understand the link between compliance management, corporate sustainability, and ESG outcomes. Their contributions provide the theoretical backbone for interpreting compliance not as a narrow legal requirement, but as a strategic enabler of corporate responsibility and long-term value creation.

Archie Carroll (1991): CSR Pyramid

Archie B. Carroll's Pyramid of Corporate Social Responsibility is one of the most influential conceptualizations of corporate responsibility. The model distinguishes four levels of responsibility:

1. Economic responsibility – ensuring profitability and efficiency, forming the base of the pyramid.
2. Legal responsibility – compliance with laws and regulations, which sets the minimum expectations for corporate conduct.
3. Ethical responsibility – going beyond legal requirements to act fairly and responsibly.
4. Philanthropic responsibility – voluntary contributions to society's well-being (Carroll, 1991).

In terms of compliance, Carroll highlights that legal responsibility is non-negotiable: organizations cannot be considered responsible if they fail to comply with regulations. However, ESG compliance expands this view, because stakeholders today expect companies to also engage with ethical and philanthropic dimensions. For example, reducing emissions in line with international climate targets may go beyond the law but reflects ethical responsibility within the ESG framework.

John Elkington (1997): Triple Bottom Line

John Elkington's Triple Bottom Line (TBL) framework extended the debate by introducing a performance model based on three pillars: people, planet, and profit (Elkington, 1997). Unlike traditional business models that prioritize financial profit, TBL emphasizes that sustainable businesses must generate value for society and the environment alongside economic returns.

In compliance management, the TBL model serves as a measurement framework. EU regulations such as the CSRD now require companies to disclose how they create value across all three dimensions. In this way, compliance mechanisms transform Elkington's theoretical idea into binding reporting obligations, ensuring accountability and comparability across firms.

Michael Porter & Mark Kramer (2011): Creating Shared Value

Michael Porter and Mark Kramer advanced the concept of Creating Shared Value (CSV), arguing that businesses can strengthen their competitiveness while solving social and environmental challenges (Porter & Kramer, 2011). Unlike traditional CSR, which often emphasized philanthropy, CSV integrates social progress into core business strategies.

From a compliance perspective, CSV demonstrates how aligning with ESG standards can become a source of competitive advantage. For instance, companies that adopt sustainable supply chain compliance practices can simultaneously reduce reputational risk and appeal to socially responsible investors. Compliance thus becomes not just a cost centre, but a driver of innovation and market positioning.

Ukrainian Scholars and Transitional Perspectives

In Ukraine, scholars have emphasized the role of compliance in transitional and post-Soviet contexts:

S. Mochernyi (2013): Focused on corporate governance in transitional economies, highlighting compliance as a structural prerequisite for sustainability. In contexts with weak institutions, compliance ensures stability, accountability, and alignment with international standards.

O. Prokopenko (2020): Concentrated on environmental policy and sustainability in Ukraine. He emphasized the compliance gaps between Ukrainian companies and EU regulations, arguing that alignment with European frameworks (e.g., CSRD, EU Taxonomy) is essential for Ukraine's integration into global markets.

These Ukrainian perspectives underscore that in transitional economies, compliance is not merely a regulatory formality but also a strategic necessity for accessing foreign investment, building trust with stakeholders, and advancing EU integration.

A conceptual diagram showing how key scholars and theories link into ESG compliance:

> Carroll (1991) → Legal/ethical responsibilities.

> Elkington (1997) → Triple Bottom Line accountability.

> Porter & Kramer (2011) → Competitive advantage via Shared Value.

> Mochernyi (2013) → Governance in transitional economies.

> Prokopenko (2020) → Compliance gaps and EU alignment.

Together, they show that compliance management is a bridge between theory and practice - translating broad concepts of responsibility into enforceable systems that shape corporate behaviour, investor trust, and societal impact.

11.4. EU and Ukrainian Examples and Cases

Compliance with ESG standards is not only a regulatory obligation but also a strategic practice that can help companies strengthen resilience, attract investment, and build

trust with stakeholders. Case studies from both the European Union and Ukraine illustrate how organizations integrate compliance management into their sustainability strategies.

Unilever (EU Case)

Unilever, one of the world's largest consumer goods companies, has become a benchmark for corporate sustainability and ESG compliance in the EU. Through its Sustainable Living Plan (2010–2020) and subsequent Compass Strategy (2021–present), Unilever aligned its business practices with EU sustainability directives, including the Non-Financial Reporting Directive (NFRD) and now the Corporate Sustainability Reporting Directive (CSRD) (Unilever, 2022).

Compliance aspect: Unilever publishes audited ESG disclosures that go beyond minimum legal requirements, ensuring credibility and alignment with the EU Taxonomy.

ESG outcomes: It reports reductions in greenhouse gas emissions, improvements in supply chain labour conditions, and sustainable sourcing initiatives.

Strategic impact: Compliance enables Unilever to strengthen its global brand identity and respond to growing consumer demand for ethical products.

This case shows how compliance management is embedded into corporate strategy, transforming sustainability into a source of innovation and competitive advantage.

DTEK (Ukrainian Case)

DTEK, Ukraine's largest private energy company, has been at the forefront of integrating ESG reporting and compliance into the Ukrainian corporate landscape. Despite operating in a transitional economy, DTEK adopted international sustainability frameworks, particularly the Global Reporting Initiative (GRI) Standards and the Sustainability Accounting Standards Board (SASB) guidelines (DTEK, 2022).

Compliance aspect: Although Ukraine does not yet legally mandate ESG reporting, DTEK voluntarily produces ESG and sustainability reports, aligning with EU standards.

ESG outcomes: The company invests heavily in renewable energy projects, including wind and solar farms, and has publicly committed to reducing carbon intensity.

Strategic impact: By aligning with international frameworks, DTEK demonstrates transparency to global investors, improving access to capital and preparing for EU integration.

This case highlights how voluntary compliance can act as a bridge for Ukrainian firms, allowing them to align with EU rules while enhancing legitimacy and stakeholder trust.

Raiffeisen Bank Ukraine

As a subsidiary of the Austrian Raiffeisen Bank International, Raiffeisen Bank Ukraine must comply with both EU banking regulations and local Ukrainian laws. The bank has introduced sustainability practices and compliance mechanisms in line with the European Banking Authority's (EBA) guidelines on ESG risk management.

Compliance aspect: The bank integrates ESG considerations into lending policies, ensuring that financing decisions are consistent with responsible banking principles.

ESG outcomes: Increased focus on sustainable finance, including green loans and socially responsible investment products.

Strategic impact: Compliance not only reduces reputational and financial risks but also positions the bank as a leader in the emerging Ukrainian sustainable finance sector.

This case demonstrates how international banking standards and EU ESG directives directly shape compliance practices in Ukraine's financial sector.

Comparative Insights

These three examples demonstrate two critical functions of compliance management in ESG:

Risk Mitigation:

> Unilever avoids greenwashing accusations by ensuring transparency in disclosures.
> DTEK reduces reputational risks by voluntarily aligning with international standards.
> Raiffeisen Bank mitigates financial and governance risks through ESG risk integration.

Opportunity Creation:

> Unilever builds consumer trust and brand value.
> DTEK secures access to ESG-focused investors and prepares for EU market integration.
> Raiffeisen Bank positions itself as a pioneer in sustainable finance in Ukraine.
> In both the EU and Ukraine, compliance is thus more than a legal safeguard—it is a strategic enabler of corporate sustainability and social impact.

Thus, both in the EU and in Ukraine, compliance performs not only a regulatory function but also serves as a strategic factor of corporate resilience and social impact.

The table 11.2 clearly shows how EU firms operate under mandatory compliance, while Ukrainian companies adopt voluntary or hybrid approaches to align with EU expectations and attract ESG-oriented investors.

Table 11.2 EU vs. Ukraine ESG Compliance Cases

Company / Region	Compliance Basis	ESG Outcomes	Strategic Impact
Unilever (EU)	Mandatory compliance with EU directives (NFRD, CSRD, EU Taxonomy).	Reduced emissions, sustainable sourcing, improved labor conditions.	Strengthened global brand identity, enhanced competitiveness.

DTEK (Ukraine)	Voluntary compliance with international frameworks (GRI, SASB), preparing for EU alignment.	Investments in renewable energy, carbon intensity reduction, publication of ESG reports.	Enhanced investor trust, improved access to international capital, readiness for EU integration.
Raiffeisen Bank Ukraine	Compliance with EU banking ESG directives (EBA guidelines) and local financial regulations.	Integration of ESG risks into lending policies, creation of green finance products.	Leadership in Ukrainian sustainable finance, reduced reputational and financial risks.

11.5. Case in Point Boxes

Case in Point 1: Volkswagen Emissions Scandal (2015)

The Volkswagen emissions scandal, often referred to as *"Dieselgate"*, remains one of the most instructive examples of compliance failure in the modern corporate world. In 2015, investigators discovered that Volkswagen had installed "defeat devices" in millions of diesel vehicles, allowing them to pass emissions tests while in reality emitting nitrogen oxides at levels many times higher than legal thresholds (Hotten, 2015).

From a compliance management perspective, this case is highly significant for several reasons. First, it demonstrates the limits of formal compliance systems when they are not reinforced by a culture of ethical responsibility. Volkswagen's engineers and executives effectively treated compliance as a hurdle to be circumvented, rather than a framework for sustainable corporate conduct. Second, the scandal underscores the interconnectedness of ESG dimensions. While the immediate violation was environmental ("E"), the deeper issues lay within corporate governance ("G"), and the ultimate victims were society at large ("S"), whose trust was severely undermined.

The consequences were profound: billions of euros in fines and settlements, significant reputational damage, and a long-lasting erosion of consumer trust. More importantly for our purposes, the case illustrates that failure in compliance is not merely a legal matter - it fundamentally undermines the credibility of ESG commitments.

Pedagogical lesson: As students of compliance and sustainability, we must recognize that genuine ESG performance cannot be achieved through superficial compliance or manipulation of reporting standards. Compliance is only meaningful when supported by internal accountability, transparency, and an organizational culture of integrity.

Case in Point 2: Naftogaz ESG Report (2022)

In contrast, Naftogaz, Ukraine's largest state-owned energy company, presents a compelling example of how compliance with ESG frameworks can serve as a transforma-

tive tool in a transitional economy. Historically criticized for opacity and inefficiency, Naftogaz took a notable step forward in 2022 by publishing its first ESG report. The report was aligned with global standards such as the Global Reporting Initiative (GRI) and demonstrated attention to the UN Sustainable Development Goals (SDGs) (Naftogaz, 2022).

From a compliance standpoint, this initiative was remarkable because it was voluntary rather than mandatory. Ukraine does not yet impose binding ESG reporting obligations comparable to the EU's CSRD. Nevertheless, Naftogaz proactively aligned itself with European standards. This move signals to investors, regulators, and the broader public that the company seeks to operate at a level consistent with international expectations.

The report detailed commitments to reduce greenhouse gas emissions, improve workplace safety, and invest in community development programs. While these disclosures may be modest in scope compared to European multinationals, their symbolic value is considerable: they illustrate the role of compliance as a pathway to integration with the EU and a mechanism for rebuilding public trust in a sector traditionally associated with opacity.

Pedagogical lesson: The Naftogaz example shows us that compliance should not be viewed merely as a regulatory burden. In transitional economies, voluntary alignment with international ESG frameworks can be a strategic tool—one that signals transparency, attracts investment, and positions a company for long-term sustainability.

Synthesis and Reflection

A comparison of the Volkswagen and Naftogaz cases (Table 11.3) demonstrates the dual nature of compliance in practice:

In the Volkswagen case, a leading multinational ignored compliance principles, leading to reputational collapse and financial penalties. It is a stark reminder that ESG compliance is indispensable for risk management.

In the Naftogaz case, a state-owned company in a transitional economy leveraged compliance voluntarily, not because it was forced to, but because it recognized its value in signalling reform and accountability.

Table 11.3 Compliance Failure vs. Compliance Progress

Dimension	Volkswagen Emissions Scandal (2015)	Naftogaz ESG Report (2022)
Context	Multinational automaker in EU markets.	State-owned energy company in Ukraine (transitional economy).
Compliance Basis	Manipulated emissions tests; deliberate non-compliance with environmental regulations.	Voluntary alignment with GRI standards and UN SDGs despite absence of national legal requirements.

ESG Impact	Environmental (E): Major emissions violations. Social (S): Loss of consumer trust. Governance (G): Weak internal accountability.	Environmental (E): Commitments to reduce GHG emissions. Social (S): Community investment and workplace safety. Governance (G): First transparent ESG reporting initiative.
Consequences	Billions in fines, reputational damage, market trust erosion.	Increased credibility, improved investor relations, alignment with EU integration goals.
Compliance Lesson	Superficial or manipulated compliance destroys long-term value.	Voluntary compliance in transitional economies can be a strategic tool for transparency and legitimacy.

Taken together, these examples reinforce the central thesis of this chapter: compliance is not a bureaucratic formality but a strategic instrument of governance, sustainability, and legitimacy. For students, policymakers, and practitioners, the task is clear: treat compliance not as the ceiling of corporate responsibility but as the foundation upon which authentic ESG performance is built.

Practical Exercises

In this section, you are invited to move from theory to practice. The following exercises are deliberately designed to cultivate your ability to analyse real-world ESG disclosures, design compliance frameworks, and critically compare reporting practices across different regulatory environments. As future managers, policymakers, or scholars, your challenge is not only to describe compliance structures but to interpret them critically, identifying strengths, gaps, and opportunities for improvement.

Exercise 1: ESG Report Review and CSRD Alignment

Objective: To examine how companies translate ESG principles into compliance disclosures.

Instructions:

> Select the most recent sustainability or ESG report of a European or Ukrainian company. Appropriate choices might include Unilever (EU), DTEK (Ukraine), Naftogaz (Ukraine), or Raiffeisen Bank (Ukraine).
> First, identify and categorize the compliance elements: environmental disclosures, social responsibility initiatives, governance structures, and risk management practices.
> Second, compare these elements against the requirements of the Corporate Sustainability Reporting Directive (CSRD, 2022). Pay attention not only to what is reported but also to how it is reported (e.g., quantitative indicators, external verification, materiality assessments).

> Finally, provide a critical judgment: is the company's disclosure fully aligned, partially aligned, or significantly below EU expectations?

Deliverable: A short analytical paper (3–4 pages) that highlights key compliance strengths and weaknesses, supported by specific examples from the report.

Pedagogical Intention: This task will strengthen your ability to navigate real ESG documents and understand the compliance obligations that shape them.

Exercise 2: Drafting a Compliance Checklist for Ukrainian SMEs

Objective: To develop practical compliance tools that bridge abstract regulation with operational management.

Instructions:

> Assume the role of a compliance officer working for a medium-sized Ukrainian enterprise preparing to enter EU markets. Your assignment is to create a compliance checklist that would guide the SME in meeting ESG disclosure expectations.
> Identify key obligations under EU law (CSRD, EU Taxonomy, NFRD legacy requirements).
> Complement these with voluntary international frameworks such as the Global Reporting Initiative (GRI), OECD Guidelines for Multinational Enterprises, and ISO 26000.
> Transform these obligations into 10–12 actionable items (e.g., "Establish an internal ESG committee," "Audit greenhouse gas emissions annually," "Publish gender diversity statistics in workforce reporting").

Deliverable: A structured checklist (2–3 pages) that could be directly applied in a corporate setting (Table 11.4).

Pedagogical Intention: This exercise forces you to operationalize theory, translating complex directives into practical management instruments. It also develops sensitivity to the resource constraints faced by SMEs in transitional economies.

Table 11.4 Sample Compliance Checklist for a Ukrainian SME Preparing for EU Markets

Category	Compliance Requirement	Actionable Step for SME	Framework / Standard Reference
Governance	Establish ESG oversight	Create an internal ESG committee reporting to the board	CSRD, OECD Guidelines
Governance	Ensure transparency	Publish annual ESG/sustainability report on company website	CSRD, GRI Standards

Environment	Carbon emissions reporting	Measure and disclose Scope 1 and Scope 2 greenhouse gas emissions annually	EU Taxonomy, GRI 305
Environment	Climate risk assessment	Conduct a climate risk analysis (physical + transition risks)	CSRD, TCFD
Environment	Resource efficiency	Track energy and water usage; adopt efficiency targets	ISO 14001, SDG 12
Social	Employee rights & diversity	Report on gender diversity, equal pay, and labour rights	CSRD, GRI 405
Social	Health & safety	Monitor workplace safety indicators (accidents, injuries)	ISO 45001, GRI 403
Social	Community impact	Report annual contributions to local communities	ISO 26000, SDG 11
Governance	Anti-corruption compliance	Adopt anti-corruption policy and training program	OECD Guidelines, GRI 205
Governance	Data protection & ethics	Ensure compliance with GDPR where applicable	EU GDPR, CSRD
Cross-cutting	External verification	Obtain limited external assurance of ESG disclosures	CSRD requirement

Comments: *This sample checklist illustrates how an SME can translate abstract compliance obligations into practical, measurable actions. Note that each step is linked to a recognized framework, underscoring that compliance is not arbitrary but grounded in established standards. For classroom purposes, students should be encouraged to customize and expand this checklist based on their chosen industry or case company.*

Exercise 3: Comparative ESG Disclosure Analysis

Objective: To compare ESG reporting practices across different regulatory and cultural contexts.

Instructions:

> Select one EU multinational corporation (for example, Siemens, BMW, or Unilever) and one Ukrainian company (such as DTEK, Naftogaz, or Kernel).
> Carefully review each firm's ESG report, with a focus on environmental, social, and governance indicators.
> Identify similarities, such as shared reliance on global frameworks (GRI, SDGs).
> Highlight differences in terms of reporting scope, level of detail, and external as-

surance mechanisms.

> Interpret these differences: are they the result of divergent regulatory obligations (mandatory vs. voluntary), differences in stakeholder pressures, or contrasting levels of institutional maturity?

Deliverable: A comparative essay (4–5 pages) that moves beyond description to interpretation, situating corporate practices within the broader context of compliance theory and EU–Ukraine regulatory convergence.

Pedagogical Intention: This task deepens your ability to conduct comparative analysis, linking practice to theory, and demonstrating how compliance structures are conditioned by broader institutional environments.

Comments: These exercises are not intended as rote tasks. They demand careful reading, critical reasoning, and academic rigor. Above all, they ask you to reflect on a central question: *to what extent is compliance a guarantee of sustainability, and when does it risk becoming a procedural formality?*

Target Questions

1. How does compliance transform ESG from voluntary initiatives into binding corporate responsibilities? Critical Angle: Does this legal shift enhance credibility, or does it risk reducing ESG to a "box-ticking" exercise? Students should weigh both sides, considering examples like Unilever (effective integration) and Volkswagen (failure despite regulation).
2. What specific challenges do Ukrainian companies face in adapting to EU ESG standards? Critical Angle: Consider barriers such as financial constraints, limited institutional support, lack of reliable data, and weak enforcement of existing standards. How might these challenges affect Ukraine's economic integration into the EU? Students should also reflect on whether voluntary compliance is sufficient to close the gap.
3. How can compliance management increase a company's social impact? Critical Angle: Students should discuss the mechanisms through which compliance translates into impact (e.g., transparent reporting, stakeholder engagement, external assurance). They may draw on cases like Naftogaz (transparency as reform) or Raiffeisen Bank Ukraine (responsible lending).

Comments: *When engaging with these questions, avoid treating compliance as purely technical or legalistic. Instead, approach it as a dynamic governance tool that mediates between law, ethics, and strategy. Your answers should connect theoretical foundations (Carroll, Elkington, Porter & Kramer, Prokopenko) with practical realities (case studies from the EU and Ukraine). Above all, demonstrate how compliance can either reinforce sustainability as a transformative agenda or risk diluting it into a perfunctory exercise.*

References for Self-Study

1. Carroll, A. B. (1991). The pyramid of corporate social responsibility: Toward the moral management of organizational stakeholders. *Business Horizons, 34*(4), 39–48. https://doi.org/10.1016/0007-6813(91)90005-G

2. DTEK. (2022). *Sustainability report.* https://dtek.com/en/sustainability
3. Dyllick, T., & Muff, K. (2016). Clarifying the meaning of sustainable business: Introducing a typology from business-as-usual to true business sustainability. *Organization & Environment, 29*(2), 156–174. https://doi.org/10.1177/1086026615575176
4. Eccles, R. G., & Klimenko, S. (2019). The investor revolution: Shareholders lead on sustainability. *Harvard Business Review, 97*(3), 106–116.
5. Elkington, J. (1997). *Cannibals with forks: The triple bottom line of 21st century business.* Capstone.
6. Friede, G., Busch, T., & Bassen, A. (2015). ESG and financial performance: Aggregated evidence from more than 2000 empirical studies. *Journal of Sustainable Finance & Investment, 5*(4), 210–233. https://doi.org/10.1080/20430795.2015.1118917
7. Hotten, R. (2015, December 10). Volkswagen: The scandal explained. *BBC News.* https://www.bbc.com/news/business-34324772
8. Kaptein, M. (2011). Toward effective codes: Testing the relationship with unethical behavior. *Journal of Business Ethics, 99*(2), 233–251. https://doi.org/10.1007/s10551-010-0646-5
9. Mochernyi, S. V. (2013). Corporate governance in transitional economies: A Ukrainian perspective. *Economic Annals, 58*(199), 45–62.
10. Naftogaz. (2022). *Sustainability and ESG report.* https://www.naftogaz.com
11. Porter, M. E., & Kramer, M. R. (2011). Creating shared value. *Harvard Business Review, 89*(1–2), 62–77.
12. Prokopenko, O. V. (2020). Environmental policy and sustainable development in Ukraine. *Environmental Economics, 11*(1), 15–24. https://doi.org/10.21511/ee.11(1).2020.02
13. Unilever. (2022). *Sustainable living plan progress report.* https://www.unilever.com/sustainable-living

Assignments for Self-Study

1. Prepare a two-page essay analysing how compliance management can enhance ESG performance in Ukrainian SMEs.
2. Develop a comparative table of EU vs. Ukrainian ESG regulations. Include gaps and recommendations.
3. Write a mini-case study (3–4 pages) on a Ukrainian company transitioning toward EU ESG compliance.

Chapter 12: Compliance Management IT Solutions (Data Protection, AI, Cybersecurity)

Learning outcomes

After successfully mastering the materials in this section, the student will be able to:

- Interpret key legislative acts governing data protection (GDPR (European Parliament and Council, 2016) – General Data Protection Regulation, Law of Ukraine «On Personal Data Protection» (Law of Ukraine No. 2297-VI, 2010) and cybersecurity (NIS2 Directive (European Parliament and Council, 2022), Law of Ukraine «On the Basic Principles of Ensuring Cybersecurity in Ukraine» (Law of Ukraine No. 2163-VIII, 2017) and their impact on corporate compliance strategies.
- Identify the potential benefits and threats associated with the use of artificial intelligence (AI) and Regulatory Technology (RegTech) tools to optimize and automate compliance control procedures;
- Design the fundamental components of an IT compliance program, in particular, formulate data handling policies, create algorithms for responding to cyber incidents, and justify criteria for selecting technological solutions.

Key words: data protection, General Data Protection Regulation (GDPR), cybersecurity, artificial intelligence (AI), Regulatory Technology (RegTech), Data Protection by Design.

Main Definitions

RegTech (Regulatory Technology) is a class of technology companies and solutions that use information technology, including cloud computing, big data, and AI, to help organizations comply with regulatory requirements in an efficient and effective manner. The main goal of RegTech is to automate and optimize compliance processes, reduce risks and costs.

Currently, Ukrainian legislation does not contain a unified and officially established definition of the term «RegTech.» This is because the concept is a relatively new industry phenomenon that has emerged at the intersection of the financial and technological spheres and is not a formal legal category.

Nevertheless, interpretations of RegTech can be found in the documents of some state institutions. For example, the National Bank of Ukraine, in its publication «Green Paper. Development of Regulatory and Supervisory Technologies in the Ukrainian Financial Market,» offers the following interpretation (National Bank of Ukraine, n.d.): «RegTech is a set of technological solutions that can be applied by legal entities to improve the effectiveness of processes for compliance with legal requirements (regulatory compliance), as well as requirements that these entities voluntarily decide to comply with (corporate compliance).»

According to the NBU's approach, RegTech is positioned as a component of FinTech that technologically helps financial organizations comply with regulatory standards.

International regulators, such as the UK Financial Conduct Authority (FCA), which is considered one of the first in this field, define RegTech as «a subset of FinTech that focuses on technologies that can facilitate regulatory compliance more effectively than existing capabilities» (Financial Conduct Authority, 2016).

Cybersecurity is the protection of the vital interests of individuals, citizens, society, and the state when using cyberspace, ensuring the sustainable development of the information society and digital communication environment, as well as the timely detection, prevention, and neutralization of real and potential threats to Ukraine's national security in cyberspace (Law of Ukraine No. 2163-VIII, 2017). In the context of compliance, cybersecurity is a critical component of protecting information assets and ensuring business continuity in accordance with legislative and regulatory requirements.

A cyberattack is a targeted (intentional) action in cyberspace carried out using electronic communications (including information and communication technologies, software, hardware, other technical and technological means and equipment) and aimed at achieving one or a combination of the following objectives: violation of the confidentiality, integrity, and availability of electronic information resources processed (transmitted, stored) in communication and/or technological systems, obtaining unauthorized access to such resources; violation of the security, stability, reliability, and normal operation of communication and/or technological systems; use of a communication system, its resources, and electronic communications to carry out cyberattacks on other cyber protection objects (Law of Ukraine No. 2163-VIII, 2017).

Cyber protection is a set of organizational, legal, engineering, and technical measures, as well as cryptographic and technical information protection measures aimed at protecting against cyber threats, ensuring cybersecurity, resilience, integrity, availability, and confidentiality of information resources in cyberspace, as well as the ability of infrastructure to process them (Law of Ukraine No. 2163-VIII, 2017).

A compliance officer is an independent specialist within an organization who is responsible for developing, implementing, and monitoring compliance with the compliance program.

Although the concept of a «compliance officer» is not formally enshrined in national legislation, having been borrowed from international business practice, Ukrainian law regulates positions with similar functions. In the Ukrainian legal field, there are two main equivalents of this position: The Anti-Corruption Officer, whose status, rights, and duties are clearly defined in the Law of Ukraine «On Prevention of Corruption» (Law of Ukraine No. 1700-VII, 2014). The National Agency for Corruption Prevention (NAZK) has developed detailed methodological recommendations for the activities of Commissioners (National Agency for Corruption Prevention, 2021).

At the same time, in the financial sector (banks, financial companies), the Law of Ukraine «On Preventing and Combating the Legalization (Laundering) of Proceeds from Crime, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction» (Law of Ukraine No. 361-IX, 2019) and the regulations of the National

Bank of Ukraine establish requirements for the appointment of a responsible employee for financial monitoring. His functions (control over compliance with legislation, risk management, reporting) largely coincide with the functions of a compliance officer.

Artificial intelligence is an organized set of information technologies that can be used to perform complex tasks by applying a system of scientific research methods and algorithms for processing information obtained or independently created during work, as well as to create and use proprietary knowledge bases, decision-making models, algorithms for working with information, and determine ways to achieve set tasks (Cabinet of Ministers of Ukraine, 2020). In this context, the term «artificial intelligence in compliance» refers to the use of AI systems (including machine learning, natural language processing, and image recognition) to perform tasks that traditionally required human intelligence, such as monitoring transactions for fraud, analyzing regulatory documents, risk assessment, counterparty verification (KYC/AML), and reporting automation.

Standards, laws, and regulations

Effective IT compliance management requires a detailed understanding of the regulatory environment in which the organization operates. The development, implementation, and use of technologies are governed by a complex interaction of international standards and Ukrainian legislation. Understanding these regulations is a prerequisite for building an effective compliance program, as they define the legal boundaries, determine responsibilities, and describe the consequences for violations.

Let's take a look at the main regulations relevant to the topic of our section.

The Law of Ukraine «On the Protection of Personal Data» (Law of Ukraine No. 2297-VI, 2010) is the main domestic law regulating the processing of personal data. Its relevance to the topic is fundamental for any company operating in Ukraine. It is currently undergoing a process of harmonization with the GDPR, which increases its significance for IT compliance.

The Law of Ukraine «On the Basic Principles of Ensuring Cybersecurity in Ukraine» (Law of Ukraine No. 2163-VIII, 2017) establishes the legal framework for the national cybersecurity system. It defines key concepts, objects, and subjects of cyber protection. Its relevance to the topic lies in establishing general requirements for the protection of information systems, especially for critical infrastructure facilities.

Law of Ukraine «On Cloud Services» (Law of Ukraine No. 2075-IX, 2022) – This is a relatively new law that regulates specific issues related to the use of cloud technologies, in particular data security and state supervision. Its relevance to the topic is growing as more and more organizations move their infrastructure to the cloud, creating new compliance challenges.

Resolutions of the Cabinet of Ministers of Ukraine and orders of the State Service for Special Communications and Information Protection of Ukraine – these subordinate acts detail the requirements of the above-mentioned laws. They establish specific technical and organizational requirements for information protection in public and private systems. Their relevance to the topic is purely practical, as they provide IT

compliance teams with clear instructions for implementation.

Regarding International and European standards, laws, and regulations related to the topic, it is worth paying attention to Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR) European Parliament and Council, 2016), which is the fundamental act of modern data protection law. Its relevance to the topic is absolute, as it establishes specific rules for any organization that processes the personal data of EU citizens. The GDPR requires the implementation of technical and organizational measures for data protection, making it a key driver for IT compliance in the areas of security, access management, and incident response.

The EU AI Act (European Commission, n.d.) deserves special attention, as it is one of the first attempts in the world to create a comprehensive regulatory framework for AI. The relevance of the EU AI Act to the topic lies in the importance of establishing compliance requirements for developers and users of AI systems, especially those belonging to the high-risk category, in the near future. This forces companies to think about the ethics, transparency, and reliability of their AI solutions today.

Directive (EU) 2022/2555 (NIS2 Directive) (European Parliament and Council, 2022) significantly strengthens cybersecurity requirements for a wide range of critical infrastructure sectors. The materials of the Directive are directly relevant to our topic, as they define mandatory cybersecurity risk management measures, incident reporting requirements, and increased regulatory oversight. For compliance management, this means the need to integrate robust cybersecurity practices into the overall management system.

ISO/IEC 27001 (International Organization for Standardization [ISO], 2022) and ISO/IEC 27701 (International Organization for Standardization [ISO], 2019) are internationally recognized standards that describe a systematic approach to information security management (27001) and confidentiality (27701). Their relevance to this topic is practical, as certification to these standards allows an organization to demonstrate due diligence and serves as proof of compliance with legal requirements, including the GDPR.

NIST Cybersecurity Framework (National Institute of Standards and Technology [NIST], 2024) – although initially a voluntary framework developed in the US, it has gradually gained global recognition. Its relevance to the topic lies in the fact that the NIST Cybersecurity Framework provides a structured, risk-based approach to cybersecurity management that companies can adapt to build their own effective protection systems.

It is important to understand that the regulatory framework in the IT sector is rapidly evolving and changing. As technology evolves faster than legislation, this requires constant monitoring of changes, participation in professional discussions, and the ability to quickly adapt compliance programs to new requirements. All of this defines the key competencies for a compliance management specialist.

List of Subchapters:

12.1 Transformation of compliance management in the context of technological challenges and digital changes.

12.2 Data protection regulation: analysis of the GDPR and its implementation in the Ukrainian legal field.

12.3 The interconnection between cybersecurity and compliance management: strategic aspects of integration.

12.4 The application of artificial intelligence technologies in compliance procedures.

12.5 The impact of the RegTech ecosystem on compliance automation: analysis of practical tools.

12.1 Transformation of compliance management in the context of technological challenges and digital change

Digital transformation has fundamentally changed the business environment, transforming traditional business models and creating new sources of data and risks. Digital transformation places new demands on the compliance function. Whereas compliance officers could previously rely on periodic audits and manual documentation checks, today, in the era of big data, cloud technologies, and the Internet of Things (IoT), this approach is ineffective and inadequate. Compliance management is shifting from a reactive model (responding to violations that have already occurred) to a proactive and predictive model (forecasting and preventing risks), made possible by the integration of IT solutions into compliance processes.

The works of domestic scientists are devoted to specific issues of compliance management development in Ukraine. For example, the works of Zhitar M., Fedina V., and Bogrintseva L. (Zhyitar et al., 2025) analyze the problems and prospects of compliance management development in the Ukrainian banking sector. The researchers analyze the challenges associated with insufficient harmonization with European standards (PSD2, GDPR), low level of digitalization, high cyber risks, and limited institutional capacity of banks, the role of digital technologies (RegTech, AI), and the integration of ESG criteria into compliance practices (Zhyitar et al., 2025). Zhyta M., Fedina V., and Bohrintseva L. propose in their scientific works an approach to integrating compliance management with digital tools to increase transparency, reduce risks, and promote post-war reconstruction.

Klymchuk O. and Babak M. (Klymchuk & Babak, 2025) argue that thanks to the latest innovative technological developments, conducting business activities has become much more convenient and efficient for enterprises. The researchers argue that, for the most part, the successful implementation of planned projects at various levels depends on the efficiency of their management, and information and communication technologies greatly facilitate management processes within optimal time frames.

Vitvitska U. and Bodnar O. (Vitvitska & Bodnar, 2024) note in their research that ensuring the cybersecurity of financial data is critical for protecting financial institutions, corporations, businesses, and government agencies from cyber threats. To achieve this goal, various programs and systems are used, including data encryption, password systems, software updates, staff training, data backup, activity monitoring, network security monitoring, password managers, intrusion detection and prevention, virtual private networks, secure

browsers, identification and access systems, cryptographic data protection, vulnerability management system monitoring and auditing, etc.

Professor Möslein F. (Marburg Law School, n.d.) and his colleagues, in their works on sustainable corporate governance in the digital age (e.g., in the collection Corporate Governance and Digitalisation, 2022), analyze how digitalization affects the responsibilities of boards of directors. They argue that oversight of digital risks (including cybersecurity and AI compliance) is becoming an integral part of management's fiduciary duties.

Research published in the Journal of Business Ethics and Business & Society in 2023-2025 actively develops the concept of «algorithmic governance.» Scholars such as Will M. and Cobbe J. (Cobbe et al., 2023) explore how automated decision-making (ADM) systems create new compliance challenges related to transparency, fairness, and accountability. Their work emphasizes that traditional compliance audit methods are insufficient for verifying complex AI «black boxes.»

Deloitte's 2023 Future of Compliance report highlights the transition to a «Compliance by Design» model, where compliance requirements are integrated into IT systems and business processes at the development stage, rather than added as an external control. This requires close cooperation between compliance officers, IT developers, and business units, which is a significant cultural and organizational challenge.

The EU banking sector was one of the first to feel the pressure of digital transformation. The PSD2 (Payment Services Directive 2) forced banks to open their APIs to third-party providers (FinTech companies), which created new risks for customer data security and required a complete overhaul of authentication and transaction monitoring systems. These changes are a striking example of how regulatory requirements drive technological modernization of compliance.

The introduction of the Diya app in Ukraine is a large-scale case of digital transformation of public services. At the same time, it has created unique challenges for compliance in the field of data protection. Ongoing discussions about security architecture, data storage, and Bug Bounty programs (searching for vulnerabilities in exchange for a reward) demonstrate that digital initiatives are inextricably linked to the need to build reliable IT compliance systems.

An example of a more local option is the use of IoT sensor systems by logistics companies on their vehicles to track routes, cargo temperature, driving style, etc. From a business perspective, this is an example of optimization. From a compliance perspective, it is a huge array of new personal data (driver location, speed, cargo condition, etc.). Compliance departments (or divisions), in conjunction with IT, must develop policies for processing this data, determine data retention periods, ensure anonymization for analytics, and obtain consent from drivers to comply with GDPR requirements (European Parliament and Council, 2016).

12.2 Data protection regulation: analysis of the GDPR and its implementation in the Ukrainian legal field

Personal data protection has become one of the most important and complex areas of compliance. The adoption of the General Data Protection Regulation (GDPR) in the EU

in 2018 set a «gold standard» for the whole world and had a significant extraterritorial effect.

Let us highlight the key principles of the GDPR that should form the basis of any compliance program:

- lawfulness, fairness, and transparency. That is, data processing must have a legal basis and be understandable to the data subject;
- purpose limitation – data must be collected for specific, clearly defined, and legitimate purposes;
- data must be accurate and kept up to date;
- data must be stored for no longer than is necessary;
- data must be protected against unauthorized access.

Of particular importance are the principles enshrined in Article 25 of the GDPR, entitled «Data protection by design and by default» (European Parliament and Council, 2016). These principles are widely known in academic and professional circles as the concepts of Privacy by Design and Privacy by Default. They require the integration of data protection measures at all stages of the development of products, services, and business processes.

As an example, in 2021, the Luxembourg Data Protection Authority (CNPD) imposed a fine of €746 million on Amazon for violating the GDPR (Amazon fined €746M for violating privacy rules, 2021). Although the details of the case were not fully disclosed, the claims concerned the system of collecting and using customer data for targeted advertising, which, according to the regulator, did not comply with the principles of transparency and lawfulness of processing. This case demonstrates the serious financial consequences of non-compliance with the GDPR.

Ukraine is in the process of updating its Personal Data Protection Act (Law of Ukraine No. 2297-VI, 2010) to bring it as close as possible to the provisions of the GDPR. Ukrainian companies, especially those operating in the EU market or using cloud services from European providers, are already required to implement the GDPR requirements. For example, Ukrainian IT outsourcing companies that develop software for European clients undergo rigorous GDPR compliance audits, introduce the position of Data Protection Officer (DPO), and conduct data protection impact assessments.

12.3 The interconnection between cybersecurity and compliance management: strategic aspects of integration

Cybersecurity and compliance must be interlinked. It is impossible to ensure compliance in the field of data protection without reliable technical and organizational cybersecurity measures. The EU's NIS2 Directive has significantly expanded the list of sectors considered critical and has established strict requirements for risk management, incident reporting, and oversight.

The modern approach to cybersecurity in compliance is based on several key concepts:

> Security measures must be proportionate to the level of risk, which requires regular risk assessment and identification of threats and vulnerabilities.

> Multiple layers of protection (network perimeter, endpoints, applications, data) must be created so that if one layer is breached, another will activate.

> A «zero trust architecture» must be implemented, i.e., a fundamental shift from a «trust but verify» model to a «never trust, always verify» model. In such an architecture, no user or device (even on the internal network) is considered trusted by default. Access to resources is granted based on strict authentication and authorization for each session.

The Cybersecurity Framework, developed by the US National Institute of Standards and Technology (NIST), is the result of summarizing best practices and research in this area (National Institute of Standards and Technology [NIST], n.d.). This document, structured around five functions (identification, protection, detection, response, recovery), has become the de facto international standard for building cybersecurity programs.

As an example, in 2020, the British regulator (an independent British body responsible for protecting privacy and freedom of information rights, ICO) fined British Airways for a large-scale data breach in 2018, which affected customer data. The investigation revealed that the company had failed to take adequate security measures to protect its network and data, in particular due to the lack of multi-factor authentication on many systems. This case is an example of the direct link between cybersecurity gaps and data protection compliance violations.

A good example of the importance of integrating cybersecurity into compliance management is the NotPetya virus attack in 2017, which caused enormous damage to Ukrainian banks, energy companies, government agencies, and private enterprises. This event demonstrated the critical importance of basic cyber hygiene, network segmentation, and incident response plans. After this attack, awareness of the importance of cybersecurity in Ukrainian business and the public sector has grown significantly.

12.4 The use of artificial intelligence technologies in compliance procedures

Artificial intelligence is actively transforming compliance management by providing powerful tools for automation, analysis, and forecasting. AI systems can already analyze millions of transactions in real time, detecting complex and atypical money laundering schemes and significantly reducing the number of false positives compared to traditional systems. Natural language processing (NLP) tools can analyze emails, chats, and calls (where legally permissible) to detect signs of insider trading, collusion, or other violations (Lunhol, 2024). AI can scan thousands of sources (legislative portals, news) to track new laws and regulations affecting the company's activities and automatically assess their impact (Lunhol, 2025).

The draft EU Regulation on Artificial Intelligence (AI Act) (European Commission, n.d.) includes a risk-based approach, dividing AI systems into four categories: unacceptable risk (prohibited), high risk (subject to strict certification and supervision), limited risk (transparency requirements), and minimal risk.

At the same time, AI systems themselves are becoming a new and complex subject for compliance, raising ethical and legal challenges. For example, in the Netherlands, the government was forced to abandon the use of the SyRI (System Risk Indication) AI system (NJCM et al. v. The State of the Netherlands, 2020), which was used to detect social benefit fraud. The court ruled that the system was discriminatory and non-transparent because it predominantly targeted poor areas and did not allow citizens to understand on what basis they had been selected for verification. This is an example of an important precedent that demonstrates the limits of AI application in sensitive areas. The SyRI case was a landmark decision. It highlighted the critical need for a «human rights impact assessment» before implementing such systems in the public sector. This precedent forces compliance departments to go beyond purely technical verification and conduct in-depth ethical and social risk analysis, especially with regard to vulnerable populations. In addition, this case directly influenced the development and interpretation of the EU AI Regulation. The requirements for transparency, data quality, human oversight, and reliability for high-risk AI systems set out in the Regulation can be seen as a direct regulatory response to the shortcomings identified in the SyRI system. For compliance professionals, this means that future compliance with the AI Act will require not only formal documentation, but also demonstrative evidence that systems are fair, explainable, and do not reproduce discrimination.

12.5 The impact of the RegTech ecosystem on compliance automation: an analysis of practical tools

RegTech is the technology industry's response to the growing complexity and cost of regulatory compliance. Instead of developing their own expensive solutions, companies are increasingly turning to specialized RegTech service providers.

The main areas of RegTech solutions include customer identification and verification (automation of document collection and verification, biometric identification, screening against sanctions lists and lists of politically exposed persons, etc.); transaction monitoring for financial transaction analysis and detection of suspicious activity; automatic generation and submission of reports to regulatory authorities in the required format; risk and control management (e.g., platforms for maintaining a risk register, assigning responsibilities, monitoring the implementation of control procedures, and conducting internal audits); management of regulatory changes, etc.

Many foreign banks, such as HSBC (Hongkong & Shanghai Banking Corporation, a British international commercial bank headquartered in London, which is the largest in Europe and one of the largest in the world in terms of market capitalization), Santander (a large international financial group and one of the largest banks in the world), Deutsche Bank (one of the largest transnational banks), are actively investing in RegTech startups

or collaborating with them to strengthen their AML/KYC (Anti-Money Laundering/Know Your Customer) processes. For example, the use of solutions from companies such as ComplyAdvantage (a leading RegTech company specializing in providing data and technology solutions to combat financial crime) or Chainalysis (a company specializing in blockchain analysis) allows banks to combat financial crime more effectively and comply with the requirements of the 5th and 6th EU Anti-Money Laundering Directives.

The Ukrainian RegTech market is actively developing, especially in the financial sector. Ukrainian banks are implementing solutions for automating financial monitoring and for transitioning to the international reporting standard ISO 20022. Companies such as YouControl and OpenDataBot, although not strictly RegTech, provide services that are actively used by compliance officers to verify counterparties. The development of the Diya ecosystem also creates potential for new RegTech solutions in the field of digital identification.

Practical exercises

Exercise 1 – Workshop «Data Protection Risk Analysis (DPIA)»

Task. Form teams. Each team will receive one of the following scenarios for developing an innovative product for analysis. Your task is to conduct a Data Protection Impact Assessment (DPIA) simulation, identify potential threats to individuals' rights and freedoms, and propose measures to neutralize them.

Scenarios to choose from:

1. FinTech startup. A mobile application that uses AI to analyze user transactions and provide personalized investment advice based on their financial habits and risk tolerance.

2. HealthTech platform. A telemedicine service that allows patients to receive remote consultations and doctors to analyze data from connected medical gadgets (e.g., smart watches, blood pressure monitors).

3. HR-Tech solution. A recruiting platform that uses AI to scan resumes, automatically conduct video interviews, and rank candidates to avoid bias.

4. Smart City initiative. An IoT-based urban traffic management system that collects data from cameras and navigators to optimize traffic flow.

DPIA algorithm.

Step 1. Determining the need for a DPIA.

Analyze whether your project meets the criteria for mandatory assessment. Does it involve large-scale processing of sensitive data (health, finance), the use of new technologies (AI, biometrics), or automated decision-making with significant consequences for people?

Step 2. Data Flow Mapping.

Describe in detail the data lifecycle in your project:

1) What categories of data are collected?

2) What methods are used for collection?

3) Where and for how long will the data be stored?

4) Who are the internal and external recipients of this data?

Step 3. Analysis of legal grounds and data minimization.

Ensure that data processing complies with the key principles of the GDPR:

1) Do you have a clear legal basis for collecting each category of data (e.g., consent, contract)?

2) Is data collection limited to the minimum necessary to achieve the stated purpose?

Step 4. Threat modeling and risk analysis.

Identify potential threats to data subjects. What could happen as a result of data leakage, unauthorized access, or a wrong AI decision (e.g., financial damage, discrimination in employment, disclosure of medical secrets)? Assess the likelihood and severity of each risk.

Stage 5. Risk mitigation action plan.

For each identified risk, propose specific measures: technical (encryption, pseudonymization, two-factor authentication, etc.); organizational (development of internal policies, staff training, conclusion of non-disclosure agreements, etc.).

Step 6. Preparation of the final DPIA report.

Prepare a summary document containing a description of the project, a risk map, and proposed measures to control them.

Exercise 2 – Crisis simulator «Responding to a data leak»

Task. Imagine that you are a compliance officer at a company whose IT product (choose one of the scenarios from the previous exercise) has been cyberattacked. The attackers have not only encrypted the customer database, but also stolen it, threatening to publish it. Develop a step-by-step response plan that includes the following phases: initial assessment and containment of the threat; activation of the incident response team (lawyers, IT security, PR); preparation and implementation of official communications to the regulator and customers; post-incident analysis to prevent recurrence.

Exercise 3 – Business game «Selecting a RegTech solutions provider»

Task. Your financial company is holding a tender for the implementation of an automated customer verification system (KYC). Create a Vendor Scorecard, a document that you will use to compare potential vendors. The scorecard should include the following criteria: technical capabilities (depth of verification, API integration), information security (ISO 27001 certification, GDPR compliance), business model (cost, transparency of rates), and market reputation.

Targeted Questions

1. Consider the case of the NotPetya cyberattack. If the requirements of the NIS2 Directive regarding risk management and incident reporting had been fully implemented in the Ukrainian companies that were attacked, what three key differences in the response scenario and consequences could we have observed?
2. Based on the concept of «zero trust architecture,» compare it with the traditional security model. How does the transition to «zero trust» change not only technical settings, but also the daily behavior and level of responsibility of an ordinary employee in an organization?
3. Imagine yourself as a member of the board of directors. What questions would you ask the development team before approving the implementation of a high-risk AI system similar to SyRI to ensure compliance with ethical and legal standards?
4. Considering the functions of Ukrainian counterparts of a compliance officer (Anti-Corruption Commissioner, responsible for financial monitoring), analyze how RegTech tools such as YouControl and OpenDataBot help fulfill these responsibilities. What are the risks of over-reliance on automated systems when checking counterparties and identifying corrupt links?

List of References for Self-study

1. *Amazon fined €746M for violating privacy rules*. (2021, July 30). Politico. https://www.politico.eu/article/amazon-fined-e746m-for-violating-privacy-rules/
2. Cabinet of Ministers of Ukraine. (2020). *Order No. 1556-r: On approval of the Concept for the Development of Artificial Intelligence in Ukraine*. https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text
3. Cobbe, J., Veale, M., & Singh, J. (2023). Understanding accountability in algorithmic supply chains. In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency* (pp. 1679–1691). Association for Computing Machinery. https://doi.org/10.1145/3593013.3594073
4. DQS. (n.d.). *Інформаційна безпека за допомогою системи. Сертифікація ISO 27001*. Retrieved August 11, 2025, from https://www.dqsglobal.com/uk-ua/sertifikujte/sertifikaciya-iso-27001
5. European Commission. (n.d.). *Regulatory framework proposal on artificial intelligence*. Retrieved August 11, 2025, from https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
6. European Parliament and Council. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Official Journal of the European Union, L 119/1. https://eur-lex.europa.eu/eli/reg/2016/679/oj
7. European Parliament and Council. (2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high*

common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union, L 333/80. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

8. Financial Conduct Authority. (2016). *Feedback statement on call for input: Supporting the development and adopters of RegTech* (FS16/4). https://www.fca.org.uk/publication/feedback/fs-16-04.pdf

9. International Organization for Standardization. (2019). *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines* (ISO/IEC Standard No. 27701:2019). https://www.iso.org/standard/71670.html

10. International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (ISO/IEC Standard No. 27001:2022). https://www.iso.org/standard/82875.html

11. Klymchuk, O. V., & Babak, M. I. (2025). Compliance management in the logistics and sales system of an enterprise. In *Building integrity and compliance in Ukraine: Challenges and prospects of European integration* (pp. 114–116). TOV "Druk."

12. *Law of Ukraine No. 1700-VII. On Preventing Corruption*. (2014). Information from the Verkhovna Rada of Ukraine, 49, 2056. https://zakon.rada.gov.ua/laws/show/1700-18#Text

13. *Law of Ukraine No. 2075-IX. On Cloud Services*. (2022). Information from the Verkhovna Rada of Ukraine, 15, 52. https://zakon.rada.gov.ua/laws/show/2075-20#Text

14. *Law of Ukraine No. 2163-VIII. On the Basic Principles of Ensuring Cybersecurity in Ukraine*. (2017). Information from the Verkhovna Rada of Ukraine, 45, 403. https://zakon.rada.gov.ua/laws/show/2163-19#Text

15. *Law of Ukraine No. 2297-VI. On the Protection of Personal Data*. (2010). Information from the Verkhovna Rada of Ukraine, 34, 481. https://zakon.rada.gov.ua/laws/show/2297-17#Text

16. *Law of Ukraine No. 361-IX. On Preventing and Combating the Legalization (Laundering) of Proceeds from Crime, Financing of Terrorism, and Financing of the Proliferation of Weapons of Mass Destruction*. (2019). Information from the Verkhovna Rada of Ukraine, 25, 297. https://zakon.rada.gov.ua/laws/show/361-20#Text

17. Lunhol, O. (2024). Review of cybersecurity methods and strategies using artificial intelligence. *Cybersecurity: Education, Science, Technology, 25*, 379–389.

18. Lunhol, O. M. (2025). Synergy of digital intelligence and artificial intelligence algorithms for effective detection of cyber threats. *Science and Technology Today, 43*, 1320–1332.

19. Marburg Law School. (n.d.). *Prof. Dr. Florian Möslein, LL.M. (London)*. Retrieved August 15, 2025, from https://www.uni-marburg.de/en/fb01/faculty/civil-law/prof-dr-florian-moslein-ll-m-london

20. National Agency for Corruption Prevention. (2021). *Professional standard "Anti-corruption officer"*. https://nazk.gov.ua/wp-content/uploads/2021/08/Profesijnyj-standart-Upovnovazhenyj-z-antykoruptsijnoyi-diyalnosti-2.2-4.pdf

21. National Bank of Ukraine. (n.d.). *Green paper: Development of regulatory and supervisory technologies in the Ukrainian financial market*. https://bank.gov.ua/admin_uploads/article/Zelena_knyga_2025_fin.pdf

22. National Institute of Standards and Technology. (n.d.). *Cybersecurity framework*. Retrieved August 17, 2025, from https://www.nist.gov/cyberframework

23. National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

24. *NJCM et al. v. The State of the Netherlands*, Case No. C/09/550982 / HA ZA 18-388 (Rechtbank Den Haag 2020). https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBDHA:2020:1878

25. Vitvitska, U. Ya., & Bodnar, O. V. (2024). The use of the latest information technologies in the financial activities of enterprises. In O. V. Olshanska & A. A. Oleshko (Eds.), *Collection of conference materials* (pp. 547–549). KNUTD.

26. Zhyitar, M., Fedina, V., & Bohrynovtseva, L. (2025). Development of compliance management in domestic banking practice. *Sustainable Economic Development, 54*, 167–173. https://doi.org/10.32782/2308-1988/2025-54-25

Assignments for Self-Study

1. Based on the case study of the 2017 NotPetya cyberattack described in the section, prepare an analytical report. In the report, reveals what gaps in compliance management and cybersecurity at Ukrainian companies allowed this attack to be so devastating. Propose 3-5 key measures that organizations should implement to comply with the requirements of the NIS2 Directive in order to minimize similar risks in the future.

2. Analyze the court precedent regarding the SyRI (System Risk Indication) AI system (NJCM et al. v. The State of the Netherlands, 2020) in the Netherlands. Write an essay in which you simulate a hypothetical situation of implementing a similar system in Ukraine to monitor social benefits. Assess the potential risks of human rights violations, discrimination, and non-compliance with Ukrainian legislation, based on the lessons learned from the SyRI case and the requirements set out in the EU AI Regulation.

3. Research the current state of the Ukrainian RegTech market using the examples given in the text (YouControl, OpenDataBot) and find 2-3 additional solutions. Prepare a business proposal (concept) for a new RegTech startup that would

solve a pressing compliance issue for Ukrainian businesses, taking into account the potential of the Diya ecosystem.

4. Imagine that you have been appointed compliance officer at a Ukrainian IT company that develops a telemedicine platform. Develop a job description for yourself, taking into account the functions described in the section and Ukrainian analogues of this position (anti-corruption officer, financial monitoring officer). Draw up a plan of action for your first 90 days, including an initial risk audit, the development of key policies, and a training plan for employees.

Chapter 13: Compliance in Multinational Corporations. Third-Party & Supply Chain Compliance

Learning Outcomes

After completing this chapter, student will be able to:

- Analyze real-world compliance challenges multinational companies face when operating under different legal, cultural, and political systems, and propose possible solutions.
- Evaluate organisational models for managing compliance and design recommendations for building a global compliance programme that balances central consistency with local effectiveness.
- Analyze how cultural models and behaviour patterns differ across countries and apply this knowledge to act effectively in compliance situations.
- Identify the critical steps of third-party and supply chain due diligence and use practical tools (e.g., checklists, risk-mapping) to manage third-party risks.

***Key Words*:** Ethnocentric, Polycentric, Geocentric Approaches, Global Integration Institutional Theory, Local Responsiveness, Multinational Enterprise (MNE), Supply Chain Due Diligence, Third-Party Risk

Main Definitions

Multinational Enterprise (MNE): a company that owns or controls the production of goods or services in at least one country other than its home country. This exposes it to a complex web of different legal, economic, and cultural systems.

Institutional Theory: a management and organizational theory that explains how companies and institutions are shaped not only by economic goals, but also by social norms, rules, laws, and cultural expectations.

Third-Party Risk: the potential threat to a company's finances, reputation, and operations that comes from its reliance on external partners like suppliers, agents, and distributors.

Due Diligence: a structured process of gathering and verifying information about a third party to assess risks before and during cooperation.

Standards, Laws, and Regulations

This chapter covers a wide range of rules that apply to MNEs, including:

1. Host Country Laws: National laws in the countries where an MNE operates (e.g., labour laws, environmental standards, tax codes).

2. Home Country Laws: Laws from an MNE's home country that apply globally (e.g., the Law of Ukraine "On Prevention of Corruption", the US Foreign Corrupt Practices Act (FCPA), the UK Bribery Act, EU sanctions).

3. International Law: Conventions and principles recognised globally (e.g., the UN Guiding Principles on Business and Human Rights).

4. Supply Chain Laws: Legislation focused on due diligence in supply chains (e.g., the German Supply Chain Due Diligence Act, EU Corporate Sustainability Due Diligence Directive, Ukraine's Law "On Public Procurement" and Law "On Environmental Impact Assessment," which set requirements for ethical sourcing, compliance, and environmental standards in procurement and production).

5. Private Standards (TPR): Rules set by non-governmental bodies (e.g., the Forest Stewardship Council (FSC), the ISEAL Alliance).

6. Specific National Rules: Unique local requirements (e.g., the Ukrainian National Bank's approval for cross-border transfers or the NACP "International Sponsors of War" list).

List of Subchapters

13.1 The Myth of the 'Borderless World' and the Balancing Act

13.2 Navigating a Maze of Rules and Cultures

13.3 Third-Party and Supply Chain Due Diligence

13.4 Building a Global Compliance Programme That Works

13.1 The Myth of the 'Borderless World' and the Balancing Act

Globalisation, with its rapid technological progress and open trade, can create the illusion of a 'borderless world'. This might tempt a Multinational Enterprise (MNE) to use a single, uniform approach everywhere it operates. However, this is a dangerous misconception. Every country has its own unique set of laws, political priorities, and cultural norms. For an MNE, this means a "one-size-fits-all" compliance strategy is not just ineffective - it's a recipe for failure.

To succeed, a company must do more than just follow the written laws of its host countries. It needs a deep understanding of local business practices, cultural traditions, and unwritten "rules of the game." This is essential for effective operations and for earning a social licence to operate. In the digital age, this challenge is even greater. Companies now act as digital mediators in global conflicts, and their decisions about data and cybersecurity have major geopolitical consequences.

Every MNE must manage a fundamental tension between two opposing goals: global integration and local responsiveness.

Global integration pushes for centralising operations and standardising products to

gain efficiency and create a single, strong brand.

Local responsiveness pushes for adapting products, marketing, and business practices to meet the unique needs and rules of each local market.

How a company balances these two pressures defines its organisational structure and its entire approach to compliance. This leads to three main operational models:

The Multi-domestic Model: The MNE acts like a portfolio of independent businesses, with each country's operation having a high degree of autonomy. This makes the company very responsive to local needs. However, it often leads to duplicated work, higher costs, and makes it hard to implement a consistent global compliance culture.

The Global Model: This model prioritises efficiency above all else. The headquarters makes all key decisions and enforces standardised processes worldwide. The main weakness is inflexibility. Local teams can become passive and demotivated, and the company may fail to notice and adapt to important local compliance risks.

The Transnational Model: This hybrid model tries to achieve both global efficiency and local responsiveness. It creates a network where resources and responsibilities are shared between headquarters and subsidiaries. While it seems ideal, it is the hardest to manage and can lead to internal conflicts over power and resources, making it difficult to maintain a clear compliance framework.

13.2 Navigating a Maze of Rules and Cultures

According *to institutional theory,* MNEs must gain legitimacy in a complex global environment. This environment includes formal state institutions (laws and regulations) as well as informal ones, like cultural norms. Increasingly, it also includes *Transnational Private Regulation (TPR).*

TPR refers to voluntary standards created by private groups, like NGOs and industry bodies. These rules often become essential for accessing markets or protecting a brand's reputation.

Case in Point: The Forest Stewardship Council (FSC), an international NGO based in Germany. The FSC is a perfect example of TPR. It sets standards for responsible forest management. While not a government body, its certification is a must-have for companies in the forestry sector that want to demonstrate their commitment to sustainability. The FSC shows how private groups can create and enforce powerful cross-border compliance rules.

This complexity is made worse by international enforcement. For example, companies in Ukraine must check transactions against EU, US, and Ukrainian sanctions lists. They must also be aware of Ukraine's "International Sponsors of War" list, which, while not a formal sanction, creates significant reputational and commercial risk by flagging companies in global due diligence databases.

The best strategy often depends on the situation. A US bank, for instance, used an *ethnocentric approach* in countries with high "cultural distance" to increase control, but

a polycentric one in competitive markets where local knowledge was key.

Case in Point: Coca-Cola and McDonald's in Diverse Markets Coca-Cola's success in Africa came from a deeply polycentric model. It empowered local entrepreneurs to run micro-distribution centres, using everything from pushcarts to canoes to reach customers. In Ukraine, McDonald's showed cultural respect by using national colours and a traditional typeface, *Rutenia*, in its branding, helping it connects with the local community.

Operating in high-risk environments, like conflict zones, presents extreme compliance challenges. The war in Ukraine, for example, has pushed many MNEs towards a *polycentric approach* out of necessity. With expatriates at risk, local staff are better able to make effective operational decisions, as they understand the local security situation and community networks.

In these situations, demonstrating commitment to the host country becomes a test of integrity. This goes beyond simple corporate social responsibility. For example, IT firms like GlobalLogic and EPAM Systems were praised for their significant financial support for Ukrainian causes. In contrast, companies seen as silent on the conflict faced public criticism. This highlights the rise of "ethical compliance" - aligning a company's actions with the values and expectations of the local society.

To manage cultural complexity, MNEs can use three main staffing approaches (Table 13.1).

Table 13.1 Ethnocentric Polycentric Geocentric (EPG) staffing approaches

Approach	Staffing Logic	Compliance Logic	Critical Insight
Ethnocentric	Hiring managers from the parent country (expatriates) for key roles. This ensures control and consistency but can lead to cultural blindness and demotivate local staff.	Global HQ rules dominate. Same code of conduct, anti-bribery, and reporting rules everywhere -even if they clash with local customs.	*Strong control but rigid.* May create resentment ("foreign rules imposed on us"). Risk of local staff ignoring rules they see as irrelevant.
Polycentric	Hiring managers from the host country. This improves local adaptation and market knowledge but can lead to fragmentation, making it hard to maintain a unified global culture.	Each country adapts compliance to local laws and norms. Local versions of codes of conduct and reporting systems.	*Flexible but fragmented.* Risks "compliance arbitrage," where subsidiaries exploit weaker rules. Harder for HQ to see the whole risk picture.

Geocentric	Hiring the best person for the job, regardless of their nationality. This is often seen as the ideal but is the most complex and expensive to manage.	A global compliance framework with core non-negotiables (e.g., anti-bribery, human rights) but adapted intelligently to local contexts.	*Ideal but complex.* Expensive, requires global-local dialogue and resources. Often the most sustainable way to balance integrity and market reality.

When multinational enterprises (MNEs) work across borders, they face not only different laws but also different cultural expectations about what is "normal" or "acceptable" in business. Culture is one of the biggest challenges in global compliance. The "Cultural Iceberg" is a helpful metaphor: for every visible cultural trait (like language or dress), there is a huge, invisible mass of values and beliefs below the surface (like concepts of time, ethics, and authority). A compliance programme that ignores the invisible parts of culture will fail.

To help managers understand and compare these differences cross-cultural scholars such as Hofstede, Hall, Trompenaars, and Meyer developed models that help managers understand differences in behavior and communication across countries.

Cultural models are not just academic theory - they are practical tools that help compliance staff predict behavior, avoid misunderstandings, and manage risks in multinational operations.

In practice, these models give compliance teams a kind of "cultural risk radar": instead of being surprised by local behavior, they can anticipate it, plan for it, and act effectively while keeping global standards intact. By using cultural models, compliance managers can anticipate risks (e.g., bribery, favoritism, silence), adapt policies and training to local norms without weakening global standards, improve communication and monitoring so rules are respected across cultures, and build stronger teams and partnerships based on cultural awareness (Table 13.2).

Table 13.2 Cultural Models for Compliance Management

Model	Dimension / Scale	Example Countries	Compliance Risk	How Compliance Staff Can Use It
Hofstede https://geerthofstede.com/culture-geert-hofstede-gert-jan-hofstede/6d-model-of-national-culture/	Power Distance	High: China, Ukraine Low: Denmark, US	Employees in high-power-distance settings may fear reporting misconduct.	Provide anonymous hotlines; stress team protection instead of individual whistleblowing.

	Uncertainty Avoidance	High: Germany, Greece Low: UK, Singapore	Strict need for detailed rules vs. flexibility.	Offer step-by-step manuals in high-UA countries; allow more principle-based policies in low-UA settings.
Hall https://medium.com/@hilaryblairdraper/edward-hall-and-his-impact-on-anthropology-94be86df6970	High vs. Low Context	High: Japan, UAE Low: Germany, US	Risk of misunderstanding compliance policies and training.	Use visuals, stories, and role plays in high-context markets; detailed written guidance in low-context ones.
Trompenaars https://www.youtube.com/watch?v=NFVMh-fifZco	Universalism vs. Particularism	Universalist: US, UK Particularist: China	Favoritism or personal ties influencing supplier selection.	Stress equal treatment for all suppliers in universalist cultures; balance trust and rules in particularist ones.
	Achievement vs. Ascription	Achievement: US, Canada Ascription: Saudi Arabia, Mexico	Status over merit may distort hiring or supplier choices.	Use objective KPIs and compliance scorecards in ascription settings.
Erin Meyer (Culture Map) https://readingraphics.com/book-summary-the-culture-map-erin-meyer/	Communication (High–Low Context)	High: Japan, Brazil Low: US, Germany	Training misunderstood or skipped.	Adapt communication: visual + relational in high-context; clear, direct in low-context.
	Feedback (Direct–Indirect)	Direct: Netherlands, Germany Indirect: Japan, Ukraine	Direct criticism can offend; indirect may hide problems.	In direct cultures, be open and firm; in indirect, give private, polite feedback.

	Trust (Task-based vs. Relationship-based)	Task: US, Denmark Relationship: China, Ukraine	Over-reliance on personal networks may bypass compliance.	In relationship-based cultures, invest in trust-building before enforcing rules.
	Decision-Making (Consensual vs. Top-Down)	Consensual: Japan, Sweden Top-down: China, France	Delayed compliance action in consensus-driven settings.	Allow extra time for decisions in consensual cultures; engage key leaders early in top-down ones.

13.3 Third-Party and Supply Chain Due Diligence

When companies do business, they rarely act alone. They buy materials from suppliers, rely on distributors to reach customers, use agents to negotiate, or hire contractors to deliver services. Each of these partners becomes part of the company's reputation and legal exposure.

If a supplier pays bribes to speed up customs clearance, if a distributor sells products in sanctioned countries, or if a contractor uses child or forced labour, regulators and the public rarely stop to separate "the company" from "its partners." Instead, the company itself is held accountable.

This is why laws in Ukraine and in other countries explicitly require companies to know their third parties: who owns them, how they behave, whether they are trustworthy. In practice, this means checking legal requirements and the reputation of every business partner before and during cooperation.

For multinational enterprises (MNEs), compliance can be especially challenging because of the size and complexity of their business. Many MNEs work with thousands of suppliers, distributors, and partners in different countries, which makes it hard to see and control everything that happens in their supply chains.

They also face the problem of dealing with many different legal systems. Something that is legal in one country may be illegal in another - for example, small "facilitation payments" are allowed in some places but considered bribery under stricter laws like the UK Bribery Act.

Cultural expectations add another layer of difficulty. A gift or favor that is seen as normal in one country may be treated as corruption or even exploitation in another.

Finally, rules are changing all the time. New sanctions, trade restrictions, and ESG (environmental, social, governance) due diligence laws are introduced quickly, especially in international business. This means companies must treat compliance as a continuous process - constantly monitoring, updating, and adapting their policies.

Case in Point: In July 2025, an Italian court placed Loro Piana, the luxury cashmere brand owned by LVMH, under judicial administration for one year due to severe labor abuses identified within its supply chain. Investigations revealed that Loro Piana had subcontracted production to intermediaries lacking manufacturing facilities, who then outsourced to illegal Chinese-run workshops. These workshops forced mostly undocumented workers to labor up to 90 hours per week for a mere €4 per hour and live on-site under deplorable conditions.

For the managers, the key lesson from the Loro Piana case is that even if a company is not directly breaking the law, it can still be held responsible for failing to control its suppliers. The court said Loro Piana had put profit ahead of ethical responsibility and therefore failed in its duty to oversee third parties. As a result, the brand will now be monitored by an external administrator until it proves it has corrected its mistakes.

Third-party and supply chain due diligence is no longer just "best practice," but increasingly mandated by laws and regulations worldwide. These vary by jurisdiction, but the trend is clear: governments are requiring companies to check their supply chains for corruption, sanctions, human rights, and environmental risks.

These laws are designed to prevent bribery, corruption, fraud, and other misconduct that often occur in global supply chains. For businesses, understanding these frameworks is not just a matter of formal compliance but also a way to protect their reputation, financial stability, and access to international markets.

Ukraine has developed its own system of anti-corruption and compliance regulations, which align more closely each year with global standards such as the U.S. Foreign Corrupt Practices Act (FCPA), the UK Bribery Act, OECD Guidelines, and the new EU Corporate Sustainability Due Diligence Directive (CSDDD) (Table 13.3). These rules require companies to conduct due diligence, monitor third parties, and implement strong internal controls. The following table summarises Ukrainian and international legal frameworks for third-party and supply chain compliance.

To make the process of managing third-party and supply chain compliance clear and practical, businesses should follow a step-by-step process. For multinational companies, the same steps apply - but with extra challenges, since they must deal with many countries, cultures, and legal systems at once.

Table 13.3 - Ukrainian and International Legal Frameworks for Third-Party & Supply Chain Compliance

Law / Regulation	Country / Region	Resource	Scope / Focus	Company Obligations	Examples of Violations (Suppliers/ Distributors)
Law on Prevention of Corruption	Ukraine	https://zakon.rada.gov.ua/laws/show/1700-18#n3	General anti-corruption framework for public & private sectors	Anti-corruption program, compliance officer, partner risk assessment, contract clauses	*Retail supply fraud:* supermarket supplier falsified contracts (UAH 500M), evading UAH 66M taxes

Criminal Code	Ukraine	https://zakon.rada.gov.ua/laws/show/2341-14?lang=en#Text	Liability for bribery/fraud via third parties	Corporate liability if intermediaries act illegally	*Rail tools fraud:* collusion with suppliers, inflated tenders, losses of UAH 11.4M
Law 4111-IX (2024) Amendments to Criminal Code	Ukraine	https://zakon.rada.gov.ua/laws/show/en/4111-20?lang=en#Text	Stronger anti-corruption oversight, company liability for bribing foreign officials	Liability for lack of supervision of third parties	*Transformer supplier scam:* shell company resold equipment at double price, UAH 94.8M loss
Law 4112-IX (2024) – Tax Code Amendments	Ukraine	https://tax.gov.ua/zakonodavstvo/podatkove-zakonodavstvo/zakoni-ukraini/79439.html	OECD-aligned anti-bribery tax provisions	Monitor third-party partners to prevent misuse of tax benefits	*Sanctions evasion:* Tekhprylad supplied goods to Russia post-2022, violating bans
NACP Guidance (non-binding)	Ukraine	https://zakon.rada.gov.ua/laws/show/z0219-22#n18	Compliance standards (whistleblowing, internal controls)	Voluntary adoption, best practice for due diligence	Often ignored in private sector - “paper compliance” without partner checks
FCPA (Foreign Corrupt Practices Act)	USA	https://www.trade.gov/us-foreign-corrupt-practices-act	Prohibits bribery of foreign officials; requires internal controls	Due diligence on agents/distributors, internal controls	*Walmart Mexico scandal:* bribes paid via third-party intermediaries to secure permits
AML / Counter-Terrorist Financing Laws The FATF Recommendations	Ukraine, EU, global	https://zakon.rada.gov.ua/laws/show/361-20#Text https://finance.ec.europa.eu/financial-crime/anti-money-laundering-and-countering-financing-terrorism-eu-level_en https://www.fatf-gafi.org/en/topics/fatf-recommendations.html	Financial & high-risk sectors	KYC, ongoing monitoring, report suspicious deals	*Mining plant case:* managers routed raw materials through related entities, embezzling UAH 400M
UK Bribery Act	UK	https://www.legislation.gov.uk/ukpga/2010/23/contents	Prohibits all forms of bribery, incl. private-to-private	Adequate procedures to prevent bribery	*Rolls-Royce case:* distributors paid bribes in multiple countries; company fined £671M

Sapin II Law	France	https://www.global-compliancenews.com/anti-corruption/handbook/anti-corruption-in-france/	Anti-corruption corporate duty	Risk mapping, supplier due diligence, whistleblowing	*TechnipFMC case:* fined €296M for using intermediaries to bribe Nigerian officials
German Supply Chain Due Diligence Act	Germany	https://www.csr-in-deutschland.de/EN/Business-Human-Rights/Supply-Chain-Act/supply-chain-act.html	Human rights & environmental risks	Supply chain mapping, risk assessments, reporting	*Clothing retailers*: linked to suppliers using forced labor in Asia (investigations ongoing)
EU Corporate Sustainability Due Diligence Directive (CSDDD)	EU	https://commission.europa.eu/business-economy-euro/doing-business-eu/sustainability-due-diligence-responsible-business/corporate-sustainability-due-diligence_en	Human rights, environmental, governance risks	Identify, prevent, mitigate adverse impacts	*Agribusiness imports*: soy supply chains tied to Amazon deforestation
UK Modern Slavery Act	UK	https://www.legislation.gov.uk/ukpga/2015/30/contents	Forced/child labor in supply chains	Annual public statement on due diligence	*Fashion sector*: suppliers exposed using child labor in textile factories
Australian Modern Slavery Act	Australia	https://www.legislation.gov.au/C2018A00153/latest/text	Forced labor in supply chains	Mandatory reporting	*Construction imports*: timber linked to illegal logging & forced labor
UFLPA	USA	https://www.cbp.gov/trade/forced-labor/UFLPA	Presumption against goods from XUAR	Prove no forced labor used	*Textiles/electronics seized*: supply chains tied to Uyghur forced labor
Conflict Minerals Rules	USA & EU	https://policy.trade.ec.europa.eu/development-and-sustainability/conflict-minerals-regulation_en https://www.sec.gov/rules-regulations/2012/08/conflict-minerals	Sourcing of tin, tungsten, tantalum, gold	Due diligence, trace chain of custody	*Tech sector*: use of minerals from armed groups in DRC without proper tracing

Step 1 – Identify. List all suppliers, distributors, agents, contractors.

Map the supply chain. Companies need to map beyond Tier 1 (the company business buys directly from, immediate suppliers) where possible to understand where their products really come from and to identify hidden risks.

Many compliance risks (child labor, environmental harm, corruption) happen deeper in the supply chain, not at Tier 1, because those lower tiers are harder to monitor.

Step 2 – Screen. Check beneficial owners, sanctions list, PEPs, adverse media. Verify company registration and licenses. The table below explains the main checks, and the tools or methods companies use to verify their partners.

Table 13.4 Tools to verify company's partners

Check Type	Why It's Done	Tools Used	Example
Screening Third Parties	To know who you're working with and reduce risk of fraud or misconduct	Questionnaires, internal databases, automated platforms like Refinitiv World-Check, YouControl, Unified Register of Debtors	Checking if a new supplier has a history of breaking contracts
Beneficial Owners	To see who really owns/controls a company	National corporate registries, Opendatabot, Unified State Register of Legal Entities, Individual Entrepreneurs, and Public Organizations (USR), shareholder documents	Finding out that a "small supplier" is owned by a big competitor
Sanctions Lists	To avoid dealing with banned individuals or companies	UN, EU, OFAC lists, automated screening tools, Liga:Zakon / ContrAgent, The State Financial Monitoring Service of Ukraine	Ensuring your company doesn't trade with someone on a sanctions list
PEPs (Politically Exposed Persons)	High-risk individuals due to political influence	PEP databases like World-Check, automated screening	Checking if a potential distributor is related to a government official
Adverse Media / Negative News	To detect reputational risks	Factiva, Meltwater, Google Alerts, news monitoring tools	Finding news that a partner was involved in bribery

Company Registration & Licenses	To confirm the company is legal and allowed to operate	Official business registers, licensing authorities, USR	Verifying that a contractor has a valid business license

Step 3 – Risk Assessment. Key Factors to Consider (Table 13.5):

Sector / Industry. Certain industries are inherently higher risk (e.g., energy, defense, construction).

Geography / Location. Countries with high corruption, weak legal systems, or sanctions exposure increase risk.

Transaction Type. Risk increases with large, complex, or politically sensitive transactions.

Government Links / PEP Exposure. Partners connected to public officials or politically exposed persons (PEPs) are high risk.

Table 13.5 Third parties risk categories

Risk Level	Description	Typical Actions
Low Risk	Partners with a clean background, low-value transactions, operating in low-risk countries/sectors	Standard contract review, basic monitoring, occasional re-screening
Medium Risk	Partners in moderately regulated sectors, higher-value transactions, or countries with some corruption or sanctions risk	Enhanced due diligence, verify beneficial owners, review licenses, occasional on-site checks
High Risk	Partners in high-risk sectors (e.g., defense, mining), high-value or politically sensitive transactions, countries with high corruption or sanctions exposure, or connected to government/PEPs	Full due diligence, detailed background checks, continuous monitoring, require approvals from senior management

Step 4 – Due Diligence. For high-risk partners: request documents, perform site visits, financial & reputation checks. Review ESG, labor, and human rights standards. Extra for MNE: Coordinate enhanced due diligence across subsidiaries to avoid gaps.

Step 5 – Contracting. Insert compliance clauses: anti-corruption, audit rights, sanctions, termination rights. Require supplier certifications.

Step 6 – Training & Communication. Train staff and suppliers on compliance rules. Share codes of conduct and reporting channels. Extra for MNE: Adapt training to local cultures and languages; include cultural intelligence.

Step 7 – Monitoring & Auditing. Re-check partners periodically, monitor invoices, deliveries, transactions. Investigate red flags and complaints.

Step 8 – Reporting & Remediation. Maintain hotlines for employees and suppliers. Investigate violations, report to regulators if needed. Apply remediation: warnings, termination, or self-reporting.

Step 9 – Review & Improve. Update policies regularly (new sanctions, ESG laws, etc.). Assess how effective due diligence processes are.

13.4 Building a Global Compliance Programme That Works

To manage all the complexities, an MNE needs a robust and dynamic global compliance programme. It must be centrally driven to ensure consistent standards but also flexible enough to be adapted locally. The essential elements are:

> Committed Leadership: A clear “tone from the top” where leaders champion integrity.

> A Clear Code of Conduct: An accessible code, translated into local languages, that addresses local risks.

> Continuous Risk Assessment: A process to constantly identify and manage compliance risks.

> Independent Oversight: A compliance function with sufficient authority and resources.

> Effective Training: Regular, tailored training for all employees and key partners.

> Confidential Reporting: A secure whistleblowing channel for raising concerns without fear of retaliation.

> Monitoring and Improvement: Proactive checks and audits to test the programme’s effectiveness and adapt it to new risks.

A career in global compliance is a challenging but rewarding path for those who enjoy problem-solving, understanding different cultures, and upholding ethical standards on a global scale. A compliance professional in an MNE is not just a rule-checker, but a strategic partner to the business. Their job is to help the company achieve its goals while navigating complex risks and maintaining its integrity. This involves:

> Advising business leaders on the risks of entering new markets.

> Investigating potential wrongdoing, such as bribery or fraud.

> Training employees and partners on ethical conduct.

- Designing systems and controls to prevent compliance failures.
- Communicating with regulators and other external stakeholders.

Key Skills for a Global Compliance Career

To succeed in this field, you need a unique blend of hard and soft skills (Table 13.6):

- Analytical Skills: The ability to interpret complex laws and data to identify risks.
- Cultural Intelligence (CQ): The capacity to work effectively across different cultures, understanding nuances in communication and business practices.
- Strong Communication: The ability to explain complex rules clearly and persuasively to diverse audiences.
- Business Acumen: A deep understanding of how the business operates and creates value.
- Unquestionable Integrity: A strong ethical compass and the courage to speak up, even when it is difficult.
- Resilience: The ability to handle pressure and manage crises effectively.

Table 13.6 Connecting Concepts to a Compliance Career

Concept from this Chapter	Real-World Task for a Compliance Professional
Global vs. Local Models	Advising on how to structure the compliance function to match the MNE's operational model (e.g., more local autonomy in a multi-domestic company).
Transnational Private Regulation (TPR)	Monitoring standards from bodies like the FSC or Fairtrade to ensure the company's supply chain meets customer and investor expectations.
Ethnocentric vs. Polycentric Staffing	Working with HR to assess the compliance risks of different staffing models for a new international office.
Third-Party Due Diligence	Conducting an in-depth investigation of a potential sales agent in a high-risk country to check for red flags related to corruption.
Ethical Compliance	Developing a community investment strategy in a host country to build trust and demonstrate the company's commitment beyond legal requirements.

Practical Exercises

Scenario Analysis: Your company is a German automotive manufacturer planning to open a new production facility in Vietnam. In small groups, discuss the potential com-

pliance challenges related to (a) supply chain management (sourcing raw materials ethically), (b) labour laws and cultural work expectations, and (c) environmental regulations. Which staffing approach (ethnocentric, polycentric, or geocentric) would you recommend for the senior management team, and why?

Role-Play: One student plays the role of a Compliance Officer for a French retail MNE. Another student plays a newly appointed local manager for the company's first store in Kyiv, Ukraine. The Compliance Officer must brief the local manager on the key compliance risks, including navigating sanctions lists, managing third-party distributor risks, and the importance of demonstrating corporate integrity in the current climate.

Due Diligence Simulation: Your team is considering a new sales agent in a country with a high score on the Corruption Perception Index. Create a checklist of due diligence steps you would take before signing a contract with this agent. What red flags would you look for?

Target Questions

1. How does the concept of Transnational Private Regulation (TPR) challenge traditional views of legal compliance that focus solely on state-based law? Provide an example other than the FSC.
2. Using the 'global integration vs. local responsiveness' framework, analyse the operational models of two well-known MNEs (e.g., IKEA and Nestlé). What are the compliance implications of their chosen strategies?
3. Discuss the ethical dilemmas an MNE might face when its home country's values (e.g., on freedom of speech or LGBTQ+ rights) conflict with the laws or cultural norms of a host country. How should a compliance programme address this?
4. Why does a "one-time" due diligence check on a third party insufficient? Explain the importance of ongoing auditing. Discuss the strong and weak sides of the compliance audit.

References for Self-Study

1. Gron, O., & Iarmosh, O. (2025). Compliance risk management as a key element of international companies' economic security. *Suchasni problemy modelyuvannya sotsial'no-ekonomichnykh system: materialy XVI Mizhnarodnoyi naukovo-praktychnoyi konferentsiyi* [Modern problems of modeling socio-economic systems: Materials of the XVI International scientific and practical conference]. Kharkiv, Ukraine.
2. Martinez, V. R. (2021). Third party and appointed monitorships. In B. van Rooij & D. D. Sokol (Eds.), The Cambridge handbook of compliance (pp. 605-615). Cambridge University Press.
3. Nezhyva, M. O., Mysiuk, V. O., & Nehodenko, V. S. (2024). Anti-corruption compliance: new business rules. *Ekonomìka, Upravlìnnâ Ta Admìnìstruvannâ*, *2(108)*, 92–102. https://doi.org/10.26642/ema-2024-2(108)-92-102

4. Shcherbakova N. V. (2025). Due diligence vs. Compliance – чи який інструмент краще забезпечує ефективність бізнесу та його фінансову стабільність. *Аналітично-Порівняльне Правознавство*, 2. https://doi.org/10.24144/2788-6018.2025.02.57

5. Byars, Stephen M. (2018). Business ethics. Houston, Texas: OpenStax, Rice University. Edited by Kurt Stanberry. https://openstax.org/details/books/business-ethics.

Assignments for Self-Study

1. *Case Study Research:* Select a multinational corporation that has recently faced a significant compliance failure related to its supply chain or a third-party relationship (e.g., corruption, human rights, environmental). Write a 1,500-word analysis of the case, identifying the root causes of the failure, the impact on the company, and evaluating the company's response.
2. *Policy Brief:* Imagine you are a consultant for an MNE planning to expand into a new region (e.g., Southeast Asia or Latin America). Develop a policy brief (750 words) outlining a cultural and ethical compliance strategy. The brief should recommend a specific staffing approach and provide guidelines for navigating local customs, gift-giving norms, and business etiquette.
3. *Comparative Analysis:* Compare and contrast the requirements of the German Supply Chain Due Diligence Act with the proposed EU Corporate Sustainability Due Diligence Directive (CSDDD). What are the key similarities and differences for an MNE operating across the EU?

Co-funded by the European Union

EUComplianceM4UA

KNOWLEDGE QUALITY SELF-ASSESSMENT CHECKLIST

Purpose of this Self-Assessment: This checklist is designed as a practical self-evaluation tool for master's students studying compliance management.

It enables students to systematically assess their own level of understanding, application, and critical thinking in compliance-related topics within the *Compliance Management: Master's Student Guidebook*.

How to Use This Checklist

> Go through each section and tick (✓) the statements that apply to you

> If unsure, leave it blank — this indicates a learning gap

> At the end, reflect on areas with missing checks

This is a self-diagnostic tool, not an exam

1. Conceptual Understanding

☐ I understand the core principles of compliance management

☐ I can clearly explain what a Compliance Management System (CMS) is

☐ I understand the role of ethics, integrity, and corporate culture

☐ I can distinguish between compliance, risk management, and governance

2. Legal and Regulatory Knowledge

☐ I am familiar with key EU regulations and compliance standards

☐ I understand basic principles of anti-corruption and AML frameworks

☐ I can explain data protection requirements (e.g., GDPR)

☐ I understand the legal consequences of non-compliance

3. Application and Practical Skills

☐ I can apply compliance concepts to real business scenarios

☐ I can identify compliance risks within an organization

☐ I can propose practical mitigation measures or controls

☐ I can connect compliance with HR, IT, and operational processes

4. Risk and Systems Thinking

☐ I understand how to conduct a basic compliance risk assessment

- ☐ I can prioritize risks based on impact and likelihood
- ☐ I understand how internal controls reduce compliance risks
- ☐ I can analyse how compliance integrates into organizational systems

5. Critical Thinking and Evaluation

- ☐ I can critically evaluate compliance policies and frameworks
- ☐ I can identify weaknesses or gaps in compliance systems
- ☐ I compare different approaches, standards, or case outcomes
- ☐ I support my conclusions with logical reasoning and evidence

6. Ethical Awareness and Professional Judgement

- ☐ I can recognize ethical dilemmas in business situations
- ☐ I consider integrity and corporate values in decision-making
- ☐ I understand the importance of “tone from the top”
- ☐ I can evaluate decisions in terms of ESG and social impact

7. Communication and Reporting

- ☐ I can clearly explain compliance issues to non-experts
- ☐ I can structure a basic compliance report or analysis
- ☐ I can communicate risks and recommendations effectively
- ☐ I use correct terminology and professional language

8. Academic and Knowledge Quality

- ☐ I use reliable and credible sources (academic, legal, institutional)
- ☐ My knowledge is up-to-date and relevant
- ☐ I critically analyse sources, not just describe them
- ☐ I properly reference and avoid plagiarism

9. Self-Reflection and Improvement

- ☐ I can identify my knowledge gaps in compliance topics
- ☐ I actively seek feedback from peers or supervisors
- ☐ I revise my work based on feedback
- ☐ I take responsibility for continuous learning

Self-Evaluation Summary
Count your checked boxes:

- **32–36** ✓ → Advanced level (ready for professional application)
- **24–31** ✓ → Proficient (strong, but some gaps remain)
- **16–23** ✓ → Intermediate (needs more application and integration)
- **Below 16** ✓ → Basic (focus on fundamentals and key concepts)

HOW TO APPLY YOUR KNOWLEDGE?

Compliance Management gives organizations tools that align the organization's operations with legal, regulatory, and ethical requirements. Applying this knowledge of compliance Management in practice means translating abstract principles into concrete processes such as internal control systems, risk assessments, and codes of conduct. For example, in the financial sector, compliance frameworks reduce exposure to money laundering, reputational damage or fraud, while in manufacturing or healthcare they ensure data protection and product safety.

For students, linking compliance to future jobs requires seeing compliance as a transversal competence that applies across industries. Whether entering banking, consulting, technology, or the non-profit sector, graduates can use compliance knowledge to strengthen their professional profile. Understanding regulations such as the EU General Data Protection Regulation (GDPR), anti-money laundering directives, or ISO standards allows students to demonstrate readiness for roles that demand accountability and ethical decision-making.

Following are concrete job profiles highlight the professional relevance of compliance:

- **Compliance Officer**: Ensures adherence to internal and external regulations by developing policies, monitoring procedures, and training employees. Key skills include regulatory expertise, analytical thinking, and clear communication.
- **Risk Analyst**: Identifies potential operational, financial, or reputational risks and proposes strategies to mitigate them. This role requires strong data analysis skills, problem-solving ability, and knowledge of risk management frameworks.
- **Ethics Consultant**: Advises organizations on ethical business conduct, corporate social responsibility, and integrity management. Competencies such as critical reasoning, intercultural sensitivity, and conflict resolution are central to this role.

Across these professions, the most important competencies include regulatory knowledge, critical and ethical judgment, communication, adaptability, and integrity. Graduates who develop both technical expertise and soft skills will be able to apply compliance knowledge effectively, ensuring that organizations remain resilient, trustworthy, and sustainable in an increasingly complex regulatory environment.

RECOMMENDED RESOURCES

1. Access to the Acquis Communautaire (the total body of European Union (EU) law). https://eur-lex.europa.eu/homepage.html?locale=en
2. Civil Law Convention on Corruption (ETS No. 174). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=174
3. Compliance Brettspiel “Integrity Now!”. https://www.equeo-compcor.de/training-sprodukte/compliance-brettspiel.html
4. COSO ERM Framework. https://www.coso.org/erm-framework
5. Country Comparison tool. https://www.theculturefactor.com/country-comparison-tool
6. Deutsche Institut für Compliance e.V. (DICO). https://www.dico-ev.de/
7. Die Daimler Truck. https://www.daimlertruck.com/
8. Die Deutsch-Ukrainische Akademische Gesellschaft e.V. – The German-Ukrainian Academic Society (DUAG). https://ukrainet.eu/
9. Ethics & Compliance Initiative (ECI). https://eci-insights.com/
10. European Securities and Markets Authority (ESMA). https://www.esma.europa.eu/
11. Foreign Corrupt Practices Act: https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act
12. German Corporate Governance Codex. https://www.dcgk.de/de/
13. DICO. https://www.dico-ev.de/behavioral-compliance-ethics/
14. Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW). https://www.idw.de/idw/idw-verlautbarungen/idw-ps-980-09-2022.html
15. International Compliance Association (ICA). https://www.int-comp.org/
16. International Organization for Standardization (ISO). https://www.iso.org/standard/37303
17. Law of Ukraine on Prevention of Corruption. https://zakon.rada.gov.ua/laws/show/1700-18?lang=en#Text
18. Organisation of Economic Co-Operation and Development (OECD). https://www.oecd.org/en.html
19. PricewaterhouseCoopers GmbH Wirtschaftsprüfungs- und Beratungsgesellschaft (PWC). https://www.pwc.de/en/about-us.html
20. Principal-Agent Problem Causes, Solutions, and Examples Explained. https://www.investopedia.com/terms/p/principal-agent-problem.asp
21. Recognizing whistleblowers. National Whistleblowing Centre. https://www.whistleblowers.org/members_categories/meet-whistleblowers/

22. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119, 4.5.2016, p. 1 et seq. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
23. The EU Artificial Intelligence Act. https://artificialintelligenceact.eu/
24. Transparency International (TI). https://www.transparency.org/en
25. UK Bribery Act: https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf
26. US Sentencing Guideline. https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/1991/manual-pdf/1991_Guidelines_Manual_Full.pdf
27. World Compliance Association. https://worldcomplianceassociation.com/
28. YouControl. https://youcontrol.com.ua/en/

Appendix 1: Compliance Management System vs. Compliance Program

Feature	Compliance Management System	Compliance Management Program
Definition	Organization-wide framework to manage compliance risks and embed ethical behavior (ISO 37301).	Specific initiatives or activities designed to address compliance requirements or risks (ECI,2016).
Scope	Holistic and continuous; covers policies, culture, risk assessment, training, monitoring, and improvement.	Narrower focus; may target a specific law, regulation, or compliance issue.
Objective	Ensure long-term compliance, integrate into corporate strategy, and foster ethical culture.	Achieve short- to medium-term compliance with particular rules or obligations.
Components	Governance & leadership, risk-based approach, policies & procedures, training & communication, monitoring & auditing, reporting & improvement (ISO 37301).	Policies, procedures, training, monitoring, and reporting—focused on specific risks (ECI).
Integration	Fully embedded in business processes and decision-making.	Often standalone or partially integrated within the organization.
Sustainability	Designed for continuous improvement and lasting impact.	Often pro/reactive or time-limited, addressing immediate compliance needs.

Appendix 2: Chief Ethics and Compliance Officer (CECO) – Job Description

Position Summary

The Chief Ethics and Compliance Officer (CECO) is responsible for developing, implementing, and overseeing the organization's ethics and compliance program. This role ensures that business operations comply with applicable laws, regulations, industry standards, internal policies, and ethical principles. The CECO acts as a trusted advisor to senior leadership and promotes a culture of integrity, transparency, and accountability across the organization.

Key Responsibilities

Program Development and Oversight. Develop, implement, and regularly update the organization's compliance program, including the Code of Conduct and policies on anti-corruption, conflict of interest, data protection, anti-harassment, environmental responsibility, and whistleblowing. Align internal policies with evolving legal requirements, industry regulations, and international standards.

Monitoring and Auditing. Conduct regular compliance audits and risk assessments to verify adherence to policies and regulations. Implement monitoring systems to detect and prevent violations (e.g., improper gifts, data breaches, harassment cases).

Advisory and Decision Support. Provide guidance to management and staff on ethical dilemmas, regulatory changes, and compliance risks. Review strategic business initiatives (e.g., mergers, new product launches, market entries) for compliance implications.

Training and Awareness. Design and deliver training programs for employees at all levels, from onboarding to advanced compliance workshops for managers. Embed compliance principles into daily business operations through clear communication, leadership modeling, and practical guidance.

Incident Management. Maintain secure and confidential channels for reporting misconduct. Ensure timely investigation of allegations, taking corrective and preventive measures as necessary. Uphold a non-retaliation policy to protect whistle-blowers.

Reporting and Communication. Report regularly to the Board of Directors, Audit Committee, or CEO on compliance status, risks, and incidents. Provide transparent updates to relevant stakeholders, both internal and external.

Qualifications and Competencies. Proven experience in compliance, legal, audit, or risk management roles (preferably in a senior capacity). Strong knowledge of relevant laws, regulations, and industry standards. Strategic thinking and problem-solving skills, with the ability to manage complex issues under pressure. High integrity, independence, and the ability to influence senior stakeholders. Excellent communication and training skills.

Bachelor's or Master's degree in Law, Business Administration, or a related field (compliance-specific certifications are an asset).

Organizational Position

Reports directly to the CEO or the Board's Audit/Compliance Committee to ensure independence and objectivity. Works closely with Legal, Internal Audit, Human Resources, and operational management.

Reference:

1. Tem Positions (2024). Chief Compliance Officer Job Description. https://www.tempositions.com/job-descriptions/chief-compliance-officer-cco/
2. Terms of Reference – Compliance Officer. https://s26.q4cdn.com/426641508/files/doc_downloads/corporate_governance/Terms-of-reference-Compliance.pdf
3. Diligent. (2024). The correlation between corporate governance & compliance. Diligent Blog. https://www.diligent.com/insights/compliance/the-correlation-between-corporate-governance-compliance

PROJECT PARTNERS

Lead partner:

Hochschule Wismar, University of Applied Sciences: Technology, Business and Design (HSW)

Project partners (EU):

Universidade Portucalense Infante D Henrique-Cooperativa de Ensino Superior Crl (UPT)

VŠCHT Praha Vysoka Skola Chemico-Technologika v Praze (VSCHT)

Wyższa Szkoła Przedsiębiorczości i Administracji w Lublinie (WSPA)

Project partners (UA):

Central Ukrainian National Technical University (CUNTU)

Izmail State University of Humanities (ISUH)

Simon Kuznets Kharkiv National University of Economics (S.KUZNETS KhNUE)

Donetsk State University of Internal Affairs (DonSUIA)

V. N. Karazin Kharkiv National University (KKNU)

Associated partner:

NGO Professional Network of Research and HE Managers in Ukraine (PNRM Ukraine)