Alliance for Qualification

Version 1.0 EN

October 2025

A4Q Syllabus

Certified Professional for AI Compliance (EU AI Act)



Copyright Notice and Disclaimer

© A4Q Copyright 2025 – Copyright Notice

All contents of this work are protected by copyright law. The use and exploitation rights are held exclusively by A4Q.
In particular, any reproduction, duplication, or redistribution of this work, in whole or in part, is strictly prohibited.
A4Q reserves the right to pursue civil and criminal legal action in the event of any infringement.

Disclaimer

The contents of this syllabus have been prepared with great care and are based, among other sources, on the legal provisions in force at the time of publication, in particular Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR) and Regulation (EU) 2024/1689 (Artificial Intelligence Act, AI Act).

This syllabus is provided for general informational and educational purposes only. The information presented may be abridged, simplified, or expressed in generalized terms and may therefore not fully reflect specific legal contexts or the most recent developments.

This syllabus does not constitute legal advice and must not be relied upon as a substitute for professional legal assessment in individual cases.

For the implementation of legal requirements or the evaluation of specific factual circumstances, it is strongly recommended to consult a qualified attorney or other appropriately authorized advisory body.

A4Q and the authors assume no responsibility or liability for the timeliness, completeness, or accuracy of the information provided, nor for any outcomes resulting from its use or interpretation.

Notice on the Use of Artificial Intelligence (AI)

Artificial Intelligence (AI) was utilized in the preparation of this syllabus.
While all AI-generated content has been reviewed and edited with the utmost care, it may nevertheless contain errors, omissions, contextual inaccuracies, or be subject to interpretation.
Please take this into account, particularly when applying the material in legal, regulatory, or compliance-related contexts.

Table of Contents

Copyright Notice and Disclaimer 2
Table of Contents 3
Version 9
0 Introduction 10
0.1 Purpose of the Syllabus 10
0.2 Exam-Relevant Learning Objectives and Cognitive Knowledge Levels 10
0.3 The “Certified Professional for AI Compliance” Examination 10
0.4 Accreditation 10
0.5 Level of Detail 10
0.6 Structure of this Syllabus 11
0.7 Business Outcomes (BOs) 12
0.8 Abbreviations 18
1 Introduction to AI Compliance & the EU AI Act 23
1.1 What Is Artificial Intelligence in the Regulatory Context 24
1.1.1 Regulatory Subdomains 24
1.1.2 Strategic and Regulatory Relevance of AI in Organizations 24
1.1.3 Historical and Legal Context 25
1.1.4 Relevance for Governance and Compliance 25
1.2 Overview of the EU AI Act 26
1.2.1 Key Principles of the AI Act 26
1.2.2 Roles and Responsibilities of Actors 27
1.3 Implementation Timeline (2024 – 2027) 27
1.4 Key Statement 28
2 Risk-Based Approach & Classification 29
2.1 Fundamental Principle of the Risk-Based Approach 30
2.2 Annex III – Automatically High-Risk AI Systems 30
2.3 Criteria for Risk Classification 33
2.4 Obligations and Measures by Risk Level 36
2.5 Risk Dynamics and Re-Assessments 40

© A4Q Copyright 2025

2.6 Risk-Based Prioritization of Measures 41
3 Global and Sectoral Regulatory Landscape (Overview) 42
3.1 Global AI Regulation: Status and Trends 43
3.2 Comparison: EU AI Act ↔ International Regulations 45
3.3 Sectoral AI Regulation and Interfaces 46
3.4 Harmonization and Strategies for Global AI Projects 46
3.5 Summary and Key Messages 47
4 Prohibited AI Practices (Art. 5 EU AI Act) 49
4.1 Overview of Prohibited Practices 50
4.2 Legal and Fundamental Rights Basis 50
4.3 Exceptions under Article 5(2)–(3) 51
4.4 Practical Awareness Measures 51
4.5 Practical Examples 51
4.6 Summary 54
5 High-Risk AI Systems and Obligations (Arts. 6–51 EU AI Act) 55
5.1 Identification of High-Risk AI Systems 56
5.2 Core Obligations for High-Risk AI Systems 57
5.3 Implementation within Organizations 59
5.4 Documentation and Evidence Obligations (Audit Readiness) 61
5.5 Example – Applying High-Risk AI Obligations in Practice 63
6 Risk Management and Quality Management Systems 65
6.1 Core Principles of AI Risk Management 66
6.2 The Risk Management Cycle According to ISO/IEC 23894 and the EU AI Act 67
6.3 Integration into Existing Management Systems 67
6.4 Documentation and Evidence Obligations 68
6.5 Governance, Roles, and Responsibilities 69
6.6 Importance of Integration for Compliance and Quality 70
7 Conformity Assessment and CE Marking 71
7.1 Fundamentals of Conformity Assessment (Art. 43 EU AI Act) 72
7.2 Contents of the Technical Documentation (Articles 11 & Annex IV) 74
7.3 CE Marking Procedure (Article 49 EU AI Act) 78

© A4Q Copyright 2025

7.4 Role of Notified Bodies 79
7.5 Registration in the EU Database for High-Risk AI Systems (Article 71) 80
7.6 Handling of Substantial Modifications (Article 43(4)) 81
7.7 Link to Quality and Management Systems 82
7.8 Practical Example: Conformity Route of an HR Screening Tool 82
7.9 Practical Recommendations 84
8 Transparency Obligations for Limited-Risk Systems (Art. 52 EU AI Act) 86
8.1 Article 52 EU AI Act – Transparency Obligations 87
8.2 Application Areas and Labeling Obligations 88
8.3 Design Recommendations for Interfaces and Labeling 90
8.4 Organizational Implementation in Companies 91
8.5 Typical Errors and Compliance Risks 92
8.6 Case Study: Labeling of Generative Content in Marketing 92
8.7 Practical Recommendations 93
9 General Purpose AI (GPAI) & Systemic Risk 95
9.1 Legal Framework: Articles 53–55 of the EU AI Act 96
9.2 Obligations of GPAI Providers 97
9.3 Systemic Risks & Governance 98
9.4 Compliance Review of External GPAI Models (Checklist) 100
9.5 Practical Example: Using an LLM in Customer Service 101
9.6 Recommendations for User Organizations 102
10 Fundamental Rights Impact Assessment (FRIA, Art. 27 EU AI Act) 104
10.1 Legal Basis and Scope of Application 105
10.2 Structure and Recommended Steps of a FRIA 105
10.3 Relationship and Integration with the Data Protection Impact Assessment (DPIA) 106
10.4 Practical Implementation of a FRIA – Step-by-Step Approach 107
10.5 Synergies with Existing Management Systems 109
10.6 Example: FRIA in Practice 109
11 Post-Market Monitoring, Reporting & Market Surveillance 111
11.1 Obligations After Market Placement (Article 61 EU AI Act) 112
11.2 Objectives of Post-Market Monitoring 113

© A4Q Copyright 2025

11.3 Contents of a Monitoring Plan 113
11.4 Serious-Incident-Reporting (Art. 62 EU AI Act) 114
11.5 Cooperation with Market Surveillance Authorities and the EU AI Office 117
11.6 Best Practice: Continuous Risk Re-Evaluation 118
11.7 Practical Example: Post-Market Monitoring and Regulatory Cooperation in Public Administration 119
12 Governance, Organization & Roles within the Company 121
12.1 Structure of an AI Governance System 121
12.2 Key Roles and Responsibilities 122
12.3 AI Governance Committee 123
12.4 Internal Policies and Control Mechanisms 124
12.5 Training and Awareness Programs 124
12.6 Interfaces with Existing Management Systems 125
12.7 Example – Governance Implementation in Practice 125
13 Minimal Risk & Voluntary Governance (“Ethical AI”) 128
13.1 Voluntary Governance under ISO/IEC 42001 129
13.2 OECD, UNESCO, and IEEE Guidelines for Trustworthy AI 129
13.3 Ethical Impact Assessment (EIA) 130
13.4 Linking Ethics, CSR, and ESG 130
13.5 Scenario: Ethical AI at a Telecommunications Provider 131
14 Audit Readiness, Audit Trails & Sanctions 132
14.1 Types of Audits and Responsibilities 133
14.2 Audit Preparation 133
14.3 Typical Audit Findings and Types of Nonconformities 136
14.4 Sanctions under the EU AI Act (Art. 71) 136
14.5 Corrective and Improvement Measures 136
14.6 Practical Case: Preparing for a High-Risk System Audit 137
14.7 Best Practices for Audit Readiness 138
15 Harmonized Standards & Presumption of Conformity 140
15.1 Definition and Function of Harmonized Standards 141
15.2 Presumption of Conformity – Legal Background 141

© A4Q Copyright 2025

15.3 Current Standards Landscape (Selection, 2025) 142
15.4 Integration of Harmonized Standards within Organizations 142
15.5 Collaboration between CEN/CENELEC and ISO in Standardization 145
15.6 Best Practices for Applying Harmonized Standards 145
16 Global Interfaces & Export Control 147
16.1 Data Export and Data Localization 148
16.2 Dual-Use Goods and Export Control 149
16.3 IP Rights and Licensing 151
16.4 Compliance in International Supply Chains 154
17 Optional – Practical Exercises & Case Studies 157
17.1 Introduction to AI Compliance & the EU AI Act 157
17.2 Risk-Based Approach and Classification 158
17.3 Global and Sector-Specific Regulatory Landscape 158
17.4 Prohibited AI Practices (Art. 5) 158
17.5 High-Risk AI Systems and Obligations (Arts. 6–51) 159
17.6 Risk Management & Quality Management Systems 159
17.7 Conformity Assessment and CE Marking 159
17.8 Transparency Obligations for Limited-Risk Systems (Art. 52) 159
17.9 General-Purpose AI (GPAI) & Systemic Risk 160
17.10 Fundamental Rights Impact Assessment (FRIA, Art. 27) 160
17.11 Post-Market Monitoring, Reporting & Market Surveillance 160
17.12 Governance, Organization & Roles 160
17.13 Minimal-Risk Systems & Voluntary Governance (“Ethical AI”) 161
17.14 Audit Readiness, Audit Trails & Sanctions 161
17.15 Harmonized Standards & Presumption of Conformity 161
17.16 Global Interfaces & Export Control 162
17.17 Optional Exercise Module – Advanced or Supplementary Practice Tasks 162
17.18 Optional Chapter – Roadmap & Readiness Assessment 2025 – 2027 162
17.19 Optional Chapter – Future Trends & Evolution of the Regulatory Framework 162
18 Roadmap & Readiness Assessment 2025–2027 163

© A4Q Copyright 2025

18.1 Building Blocks of an AI Compliance Roadmap 164
18.2 Typical Quick Wins and Priorities 164
18.3 Self-Assessment of AI Compliance Maturity 166
18.4 Tools and Resources for Roadmap Development 167
18.5 Conclusion 168
19 Future Outlook & Evolution of the Regulatory Framework 170
19.1 European Institutions and Governance Structures (Timeline 2025–2030) 171
19.2 Frontier AI and Systemic Risk (Time Horizon 2025–2030) 172
19.3 Expected Evolution of the AI Act (2025–2030) 173
19.4 Global Trends and International Convergence (2025–2030) 174
19.5 Strategic Implications for Organizations (Time Horizon 2025–2030) 175
19.6 Recommended Focus Areas for Further Development (2025–2030) 176
20 Recommendations for Training Providers 178
21 Learning Objectives and Cognitive Learning Levels 181
22 Literature 183
22.1 Professional Literature 183
22.2 Academic and Industry Reports 184
22.3 Legal Frameworks and Strategic Documents 185
22.4 International Standards and Technical Specifications 187
22.5 International AI Ethics and Governance Frameworks 188
22.6 Cybersecurity Threat Landscape (AI Context) 189
23 Appendices 190
23.1 Appendix A – International Provider Guidance 190

© A4Q Copyright 2025

Version

Revision History

Version	Date	Comment
1.0	October 28, 2025	Internally reviewed document with extensive updates and expansions

The current version of this document is Version 1.0 EN, build 1.003.

This document has been officially published by A4Q GmbH.

© A4Q Copyright 2025

0 Introduction

0.1 Purpose of the Syllabus

This syllabus defines the intended Business Outcomes, Learning Objectives, and core concepts of the Certified Professional for AI Compliance (EU AI Act) training and certification program.

0.2 Exam-Relevant Learning Objectives and Cognitive Knowledge Levels

Learning Objectives (LOs) support the Business Outcomes (BOs) and serve as the foundation for the Certified Professional for AI Compliance certification examination.

Participants are expected to recall content from each chapter of the syllabus, demonstrate understanding, apply knowledge, and analyze practical scenarios.

The Knowledge Levels (K-levels) assigned to each Learning Objective are indicated at the beginning of every chapter and classified as follows:

- **K1 – Remember:** Recall and reproduce facts, terminology, and basic information.
- **K2 – Understand:** Comprehend, interpret, and explain meanings and relationships.
- **K3 – Apply:** Use knowledge in specific contexts or to solve defined tasks or problems.

0.3 The “Certified Professional for AI Compliance” Examination

The *Certified Professional for AI Compliance* examination is based on this syllabus.
Answers to exam questions may require integrating knowledge from multiple sections of the syllabus.
All sections of this syllabus are relevant to the examination, **except for the Introduction and Annexes**.
Standards, books, and legal texts may be referenced; however, their content is only relevant to the exam insofar as it is summarized or cited within this syllabus.

The examination consists of **40 multiple-choice questions**. Each correct answer is worth **one point**.
A minimum score of **65%** (i.e., at least **26 correctly answered questions**) is required to pass.
The examination duration is **60 minutes**.
If the candidate’s native language is different from the language of the exam, **an additional 25% of time (15 minutes)** may be granted.

0.4 Accreditation

Training providers who wish to offer courses based on this syllabus must be accredited by A4Q and are required to use the official training materials.

0.5 Level of Detail

This syllabus consists of:

© A4Q Copyright 2025

- Business Objectives, which define the competencies participants are expected to acquire in order to address organizational challenges effectively,
- where applicable, lists of key terms that participants are required to explain,
- learning objectives for each knowledge area, describing the expected cognitive learning progression,
- and a description of the core concepts, including references to authoritative sources such as recognized professional literature and standards.

This syllabus does not aim to provide exhaustive coverage of the entire domain of AI compliance; rather, it reflects the level of detail addressed within the associated training and certification program.

.

0.6 Structure of this Syllabus

Note on the Time Structure of the Curriculum

The curriculum consists of 16 chapters containing content relevant to the certification exam, supplemented by three additional bonus chapters that provide optional learning material and are not exam-relevant.
Each chapter includes a time indication for the recommended duration of instruction, which refers to the chapter as a whole.
There is no further breakdown of time allocation within the chapters; a finer level of granularity at the subchapter level is not intended.

For the training course, the curriculum provides for approximately **16 hours of instruction**.
These hours are distributed across the individual chapters and may include additional practical exercises.
The actual instructional time required may vary depending on the participants' prior knowledge, interests, and areas of focus.

The indicated times serve as guidance for training design and enable structured preparation for the certification examination.
They do not represent minimum or maximum durations and do not replace the trainer's own didactic or methodological course planning.

Overview of Instructional Time per Chapter

No.	Chapter	Instruction Time (min)
1	Introduction to AI Compliance & the EU AI Act	45
2	Risk-Based Approach & Classification	60
3	Global and Sectoral Regulatory Landscape	70

© A4Q Copyright 2025

No.	Chapter	Instruction Time (min)
4	Prohibited AI Practices (Art. 5)	50
5	High-Risk Systems (Art. 6–51)	120
6	Risk Management & QMS (ISO 42001 / 23894)	60
7	Conformity Assessment & CE Marking	80
8	Limited-Risk & Transparency Obligations (Art. 52)	90
9	GPAI & Systemic Risk (Art. 53–55)	75
10	FRIA (Fundamental Rights Impact Assessment)	45
11	Post-Market Monitoring & Market Surveillance	60
12	Governance & Corporate Organization	45
13	Minimal Risk & Voluntary Governance	40
14	Audit Readiness & Sanctions	30
15	Harmonized Standards & Conformity	30
16	Global Interfaces & Export Control	60
17	Practical Exercises & Case Studies	–
18	Roadmap & Readiness Assessment 2025–2027	–
19	Future Outlook & Framework Development	–
Total		**960 min = 16 h ≈ 2 days**

0.7 Business Outcomes (BOs)

The Business Outcomes of this curriculum describe the intended competencies that participants are expected to acquire or further develop during the two-day training course.

They are deliberately formulated as competency-oriented rather than performance-assertive.

© A4Q Copyright 2025

As “AI Compliance” represents a broad, multidisciplinary, and dynamically evolving field, a two-day course cannot provide exhaustive or fully applicable expertise in all aspects.

The primary goal is to prepare and sensitize participants so that they understand the key principles, roles, and obligations of the EU AI Act, can assess related risks, and identify appropriate compliance measures within their professional context.

The following Business Outcomes (BOs) are addressed in the chapters of this syllabus:

Chapter	BO No.	Business Outcome (with Organizational Benefit)
Introduction to AI Compliance & the EU AI Act	**BO 1.1**	Identify organizational areas affected by the EU AI Act and contribute to establishing compliance strategies.
	BO 1.2	Participants are prepared to promote accountability and awareness of AI compliance within their organization to support early risk detection.
Risk-Based Approach & Classification	**BO 2.1**	Participants acquire the competence to classify AI systems according to the four risk levels and derive corresponding compliance obligations.
	BO 2.2	Participants are prepared to plan appropriate mitigation measures and set priorities based on the level of risk.
Global and Sectoral Regulatory Landscape	**BO 3.1**	Participants develop an understanding of international AI regulations and are capable of applying them to global projects.
	BO 3.2	Participants are prepared to identify and leverage harmonization opportunities between EU and non-EU regulatory frameworks.
Prohibited AI Practices (Art. 5)	**BO 4.1**	Participants develop awareness of prohibited AI practices and can identify such practices within their organizational environment.
	BO 4.2	Participants are prepared to assess and implement exceptions under Article 5.
High-Risk Systems & Obligations (Art. 6–51)	**BO 5.1**	Participants acquire the ability to identify relevant obligations for high-risk AI systems, support their practical implementation within the organization, and contribute to legal compliance.
	BO 5.2	Participants are sensitized to create audit-ready documentation and evidence to enhance audit preparedness.

© A4Q Copyright 2025

Chapter	BO No.	Business Outcome (with Organizational Benefit)
Risk Management & QMS (ISO 42001 / 23894)	**BO 6.1**	Participants are prepared to contribute to the establishment or adaptation of an AI risk management system in accordance with ISO/IEC 42001.
	BO 6.2	Participants gain an overview of how integrating AI processes into existing management systems (QMS, ISMS, DSMS) contributes to compliance and quality assurance.
Conformity Assessment & CE Marking	**BO 7.1**	Participants develop an understanding of conformity assessment routes and are prepared to support their application.
	BO 7.2	Participants are capable of assisting with CE marking procedures and EU database registrations.
Limited-Risk & Transparency Obligations (Art. 52)	**BO 8.1**	Participants are prepared to apply transparency requirements for chatbots, emotion recognition, and deepfakes.
	BO 8.2	Participants acquire the competence to evaluate and adapt labeling systems within interface design.
GPAI & Systemic Risk (Art. 53–55)	**BO 9.1**	Participants are prepared to analyze GPAI provider obligations and identify compliance gaps.
	BO 9.2	Participants are capable of assessing the use of external GPAI models (e.g., LLMs, generative systems) within their organization regarding transparency, risk, and compliance, and deriving corresponding recommendations.
FRIA (Fundamental Rights Impact Assessment)	**BO 10.1**	Participants are prepared to structure a FRIA and integrate it into decision-making processes.
	BO 10.2	Participants are capable of linking FRIA processes with Data Protection Impact Assessments (DPIA) and leveraging synergies.
Post-Market Monitoring & Market Surveillance	**BO 11.1**	Participants develop an understanding of post-market processes and are prepared to implement monitoring plans.
	BO 11.2	Participants are prepared to cooperate with supervisory authorities and the AI Office.

© A4Q Copyright 2025

Chapter	BO No.	Business Outcome (with Organizational Benefit)
Governance & Corporate Organization	**BO 12.1**	Participants are prepared to contribute to defining roles and responsibilities within the AI governance structure.
	BO 12.2	Participants are capable of developing internal training and policy programs to promote a culture of compliance.
Minimal Risk & Voluntary Governance	**BO 13.1**	Participants develop awareness of voluntary governance approaches in line with ISO/IEC 42001 and OECD AI principles.
	BO 13.2	Participants are prepared to align ethical guidelines with CSR and ESG objectives.
Audit Readiness & Sanctions	**BO 14.1**	Participants are prepared to plan and conduct internal and external audits in a structured manner.
	BO 14.2	Participants are sensitized to implement corrective and improvement measures derived from audit results.
Harmonized Standards & Presumption of Conformity	**BO 15.1**	Participants develop an understanding of the role of harmonized standards as compliance evidence.
	BO 15.2	Participants are prepared to assess current standards and support their application in projects.
Global Interfaces & Export Control	**BO 16.1**	Participants are prepared to evaluate risks arising from data exports, dual-use items, and intellectual property rights.
	BO 16.2	Participants are prepared to support compliance requirements within international supply chains.
Optional: Practical Exercises & Case Studies	**BO 17.1**	Participants acquire applied competence in performing risk classification, FRIA, and GPAI compliance activities.
	BO 17.2	Participants are capable of developing compliance artifacts such as documentation, labeling, and monitoring plans.
Optional: Roadmap & Readiness Assessment 2025–2027	**BO 18.1**	Participants are prepared to create an AI compliance roadmap with implementation priorities.

© A4Q Copyright 2025

Chapter	BO No.	Business Outcome (with Organizational Benefit)
	BO 18.2	Participants are capable of assessing their organization's AI Act readiness maturity level.
Optional: Future Outlook & Regulatory Evolution	**BO 19.1**	Participants develop awareness of emerging trends (e.g., Frontier AI, AI Safety Institutes).
	BO 19.2	Participants are prepared to plan and communicate strategic adjustments for future regulatory cycles.

Mapping of AI Act Requirements to Business Outcomes (BOs)

The Business Outcomes correspond to the requirements established by the EU AI Act.
All essential requirements – including those applicable to high-risk AI systems – are covered in principle.

Matrix: Business Outcomes ↔ EU AI Act Articles

Chapter / BO	Relevant EU AI Act Articles / Sections	Covered Topics / Requirements
BO 1.1 – 1.2 Introduction to AI Compliance & the EU AI Act	Arts. 1–3 (Subject Matter, Scope, Definitions) + Art. 4 (Principles of AI Systems)	Scope of application, definition of AI system, roles (provider, deployer, importer, distributor), core principles, and responsibilities.
BO 2.1 – 2.2 Risk-Based Approach & Classification	Art. 6 (Classification of AI Systems as High Risk) + Annex III (Domains) + Arts. 7–8 (Updates & Transparency on Classification)	Risk categorization, Annex III domains, thresholds, re-classification, and handling of multiple risk levels.
BO 3.1 – 3.2 Global & Sectoral Regulatory Landscape	Recitals 13–15, 81 ff.; Arts. 88–92 (International Cooperation & AI Office Mandate)	Global harmonization, international cooperation, comparison with non-EU regimes, and regulatory convergence.
BO 4.1 – 4.2 Prohibited AI Practices	Art. 5 (Prohibited AI Practices) + Recitals 31–34	Identification and exclusion of prohibited practices (manipulation, social scoring, emotion recognition, real-time biometrics). Exceptions for law enforcement.
BO 5.1 – 5.2 High-Risk Systems & Obligations	Arts. 9–15 + Arts. 16–23	Full set of obligations: risk management, data governance, technical documentation, logging, transparency, human oversight,

© A4Q Copyright 2025

Chapter / BO	Relevant EU AI Act Articles / Sections	Covered Topics / Requirements
		robustness & cybersecurity, quality management system.
BO 6.1 – 6.2 Risk Management & QMS	Art. 9 (Risk Management) + Arts. 17–23 (Quality Management System & Provider Obligations) + ISO/IEC 42001 reference	Establishing an AI management system, integration with existing corporate QMS, documentation and evidence management.
BO 7.1 – 7.2 Conformity Assessment & CE Marking	Arts. 43–51 (Conformity Assessment & CE Marking) + Annex VII (Procedures)	Internal and external conformity procedures, notified bodies, declarations of conformity, CE label, EU database.
BO 8.1 – 8.2 Limited-Risk & Transparency Obligations	Art. 52 (Transparency Obligations for Certain AI Systems)	Labeling and disclosure duties for chatbots, emotion recognition, deepfakes, and synthetic content.
BO 9.1 – 9.2 GPAI & Systemic Risk	Arts. 53–55 (General-Purpose AI & Systemic Risk Models) + Art. 56 (Codes of Practice)	GPAI obligations, transparency reports, copyright statements, evaluation, red-team testing, and incident reporting.
BO 10.1 – 10.2 FRIA (Fundamental Rights Impact Assessment)	Art. 27 (FRIA) + Recitals 73–78	Obligation for public authorities and certain private entities, linkage with DPIA, and documentation template.
BO 11.1 – 11.2 Post-Market Monitoring & Market Surveillance	Arts. 61–65 (Post-Market Monitoring & Corrective Actions) + Arts. 67–70 (Market Surveillance)	Post-market monitoring plan, incident notification, reporting, corrective actions, and cooperation with authorities.
BO 12.1 – 12.2 Governance & Corporate Organization	Arts. 17–23 (Provider Responsibilities) + Arts. 29–31 (Deployer / Distributor / Importer Obligations)	Internal roles, responsibilities, training requirements, escalation mechanisms, and organizational anchoring.
BO 13.1 – 13.2 Minimal Risk & Voluntary Governance	Recitals 60–63 + Art. 69 (Voluntary Codes of Conduct)	Promotion of ethical self-regulation, voluntary measures aligned with ISO 42001 / OECD principles, CSR / ESG integration.

© A4Q Copyright 2025

Chapter / BO	Relevant EU AI Act Articles / Sections	Covered Topics / Requirements
BO 14.1 – 14.2 Audit Readiness & Sanctions	Arts. 71–74 (Enforcement & Penalties) + Art. 63 (Post-Market Reporting)	Audit preparation, penalties, corrective procedures, and authority communication.
BO 15.1 – 15.2 Harmonized Standards & Presumption of Conformity	Arts. 40–42 (Harmonized Standards & Common Specifications)	Presumption of conformity, standardization processes (CEN / CENELEC), standard mapping to ISO 42001 / 23894.
BO 16.1 – 16.2 Global Interfaces & Export Control	Arts. 88–92 (International Cooperation) + GDPR Chapter V (Data Transfers) + Dual-Use Regulation (EU 2021/821)	Data export, third-country transfers, supply-chain compliance, IP, and trade restrictions.
BO 17.1 – 17.2 Practical Exercises & Case Studies	Arts. 6–55 (Cross-Chapter) + Annex III	Practical application of obligations (Annex III, GPAI, FRIA). Hands-on compliance documentation.
Optional BO 18.1 – 18.2 Roadmap & Readiness Assessment 2025–2027	Arts. 84–87 (Implementation Timeline & Transition Periods) + Art. 90 (AI Office Tasks)	Implementation planning, readiness evaluation, internal self-assessment, and reporting.
Optional BO 19.1 – 19.2 Future Outlook & Regulatory Evolution	Recitals 91–99 + Arts. 88–92 (AI Board, Cooperation, Future Updates)	Monitoring new guidelines, frontier-AI risks, AI Safety Institutes, and future adaptations.

0.8 Abbreviations

Abbreviation	Full Term	Meaning / Context
AI	Artificial Intelligence	Overarching topic of the syllabus
AI Act	EU Artificial Intelligence Act	EU regulation governing artificial intelligence systems

© A4Q Copyright 2025

Abbreviation	Full Term	Meaning / Context
AI Office	European Artificial Intelligence Office	EU authority responsible for enforcing the AI Act
AI Officer	Artificial Intelligence Compliance Officer	Role responsible for overseeing compliance with AI-related requirements
AI RMF	Artificial Intelligence Risk Management Framework (NIST)	U.S. framework for managing AI-related risks
AI Safety Institute (AISI)	AI Safety Institute	Planned EU/UK institution for AI safety assessments
AI System	Artificial Intelligence System	Technical system providing AI functionality
AI Trust Label	AI Trust Label	Planned EU label for trustworthy AI systems
Annex III	Annex III of the EU AI Act	List of AI systems automatically classified as “high-risk”
Art.	Article	Reference to article numbers in the EU AI Act or other EU regulations
BO	Business Outcome	Overarching learning or result-oriented unit within the syllabus
CE	Conformité Européenne	EU conformity marking for products
CE-marking	Conformité Européenne Marking	EU label indicating product conformity
CEN	Comité Européen de Normalisation	European Committee for Standardization
CENELEC	Comité Européen de Normalisation Électrotechnique	European Committee for Electrotechnical Standardization
CRA	Cyber Resilience Act	EU regulation on cybersecurity for digital products
CSR	Corporate Social Responsibility	Corporate responsibility for social and environmental issues
Data Act	EU Data Act	EU regulation on the use and sharing of data
DPA	Data Processing Agreement	Contract governing personal data processing

© A4Q Copyright 2025

Abbreviation	Full Term	Meaning / Context
DPO	Data Protection Officer	Role required under the GDPR for data protection oversight
DSA	Digital Services Act	EU regulation governing digital services
DSFA	Data Protection Impact Assessment	GDPR instrument for assessing data protection risks
DSGVO	General Data Protection Regulation (GDPR)	EU regulation on personal data protection (German: Datenschutz-Grundverordnung)
ENISA	European Union Agency for Cybersecurity	EU agency responsible for cybersecurity
ESG	Environmental, Social, and Governance	Sustainability and ethical criteria for corporate governance
EU	European Union	Political and legal organization of European member states
EU AI Board	European Artificial Intelligence Board	Coordination body of national AI authorities
FRIA	Fundamental Rights Impact Assessment	Assessment of fundamental rights under Article 27 of the AI Act
GDPR	General Data Protection Regulation	EU regulation for data protection and privacy
GPAI	General Purpose Artificial Intelligence	General-purpose AI models with multiple functions
HLEG	High-Level Expert Group on AI	EU expert group on trustworthy artificial intelligence
HR	Human Resources	Corporate personnel management
HR-System / HR	Human Resources System	HR systems, e.g., AI applications in recruitment processes
IEC	International Electrotechnical Commission	International standards organization for electrotechnical matters
IP	Intellectual Property	Intellectual property rights

© A4Q Copyright 2025

Abbreviation	Full Term	Meaning / Context
IPCT/XMP	Metadata Standards	Standard formats for technical metadata (used in AI labeling)
ISMS	Information Security Management System	Information security management framework (ISO/IEC 27001)
ISO	International Organization for Standardization	International organization for standardization
ISO/IEC 22989	Artificial Intelligence – Concepts and Terminology	Foundational standard for AI terminology and concepts
ISO/IEC 23053	Framework for Machine Learning (ML)	Framework standard for machine learning systems
ISO/IEC 23894	Artificial Intelligence — Risk Management	Standard for AI risk management (ISO/IEC)
ISO/IEC 42001	Artificial Intelligence Management System	International standard for AI management systems
ISO/IEC JTC 1/SC 42	Joint Technical Committee 1, Subcommittee 42	ISO/IEC committee for AI standardization
JSON-LD	JavaScript Object Notation for Linked Data	Format for machine-readable data labeling
K1–K6	Bloom's Taxonomy Knowledge Levels	Cognitive knowledge levels for learning objectives (Remember–Create)
KPI	Key Performance Indicator	Metric used to measure performance
LLM	Large Language Model	AI-based language model (e.g., ChatGPT, Gemini)
ML	Machine Learning	Subfield of AI focused on data-driven pattern recognition
NIST	National Institute of Standards and Technology	U.S. national standards and technology organization

© A4Q Copyright 2025

Abbreviation	Full Term	Meaning / Context
NIST AI RMF	NIST Artificial Intelligence Risk Management Framework	U.S. framework for managing AI risks
NLP	Natural Language Processing	AI method for understanding and generating human language
OECD	Organisation for Economic Co-operation and Development	International organization for economic cooperation
OECD AI Principles	Principles on Artificial Intelligence	International principles for trustworthy AI
PIMS	Privacy Information Management System	Privacy management system (ISO/IEC 27701)
QA	Quality Assurance	Process ensuring quality and consistency
QM	Quality Management	Systematic quality assurance (ISO 9001)
Red-Team-Testing	Red Team Testing	Security testing method simulating adversarial attacks
RMF	Risk Management Framework	Framework for systematic risk management
SLA	Service Level Agreement	Contract defining service quality and performance terms
UI	User Interface	User-facing component of a system (e.g., for AI labeling)
UN	United Nations	International organization and regulatory body
UX	User Experience	User perception and interaction; relevant for transparency obligations
WORM	Write Once, Read Many	Technical safeguard ensuring data immutability

© A4Q Copyright 2025

1 Introduction to AI Compliance & the EU AI Act

Duration & Objective

⏱ Instruction time: 45 minutes

🎯 **Business Outcomes:**

- **BO 1.1:** Identify organizational areas affected by the EU AI Act and contribute to establishing compliance strategies.
- **BO 1.2:** Participants are prepared to understand the key terms, roles, and objectives of the EU AI Act and to promote accountability for AI compliance within their organizations.

Learning Objectives (LO)

- **LO 1.1 (K1):** Participants recognize the fundamental importance of artificial intelligence as a key technology and can define the term and its main domains (machine learning, rule-based systems, etc.).
- **LO 1.2 (K2):** Participants explain how AI influences strategic value creation and, at the same time, introduces new compliance and risk areas within organizations.
- **LO 1.3 (K2):** Participants describe the objectives and core principles of the EU AI Act as well as the key stakeholder roles (provider, deployer, importer, etc.).
- **LO 1.4 (K3):** Participants position the EU AI Act within its temporal and organizational context and derive initial implications for their own business processes and governance structures.
- **LO 1.5 (K1):** Participants know the scope of the EU AI Act, including the distinction between AI systems developed inside and outside the EU and its applicability to providers and deployers.

Key Terms:

Artificial Intelligence (AI), Machine Learning (ML), rule-based systems, EU AI Act, provider, deployer, importer, distributor, AI Office, AI Board, risk-based approach, fundamental rights, compliance, governance, accountability, transparency obligation, scope, key technology.

Introduction

This chapter provides a foundational introduction to artificial intelligence and its growing relevance for organizations, the economy, and society. It builds a shared understanding of key terms and concepts and explains why the responsible and compliant use of AI is becoming increasingly important. This forms the basis for understanding later topics such as risk classification, governance, and compliance obligations.

© A4Q Copyright 2025

1.1 What Is Artificial Intelligence in the Regulatory Context

Artificial Intelligence (AI) refers to IT systems that perform tasks that normally require human intelligence – such as pattern recognition, natural-language processing, or decision-making.
Legally, the EU AI Act (Art. 3 (1)) defines AI as a system that, through machine learning, logic- or knowledge-based, or statistical approaches, generates outputs that influence physical or virtual environments.
This legal definition differs from purely technical descriptions: it focuses on **function and impact** rather than on a specific technology.
Its intent is to encompass all systems that generate decisions or content having legal, economic, or social effects for humans – regardless of whether they use neural networks, decision trees, or simple rule-based methods.

1.1.1 Regulatory Subdomains

- The EU AI Act does not differentiate between technologies but assesses systems based on risk potential and context of use. Nevertheless, typical development approaches can be classified from a regulatory perspective:
- **Rule-based systems** – follow fixed if-then rules. Usually minimal- or low-risk if no automated, person-related decisions are made.
- **Machine Learning (ML)** – systems learn from data; they become regulatory-relevant when training data contains bias or when decision processes lack explainability.
- **Deep Learning / Neural Networks** – often classified as high-risk under the AI Act when used for safety-critical or fundamental-rights-sensitive functions.
- **NLP & Computer Vision** – subject to the same requirements (Art. 10 data quality; Arts. 13–15 transparency and oversight) whenever personal or safety-critical data are processed.

1.1.2 Strategic and Regulatory Relevance of AI in Organizations

AI is no longer a purely technical topic but a governance-relevant business factor – offering opportunities for innovation as well as obligations for compliance and oversight.
The EU AI Act, GDPR, product-safety law, and sector-specific regulations (e.g., medical-device, financial, and labor law) are interconnected.

© A4Q Copyright 2025

Perspective	Relevant Aspects from a Business Viewpoint
Value Creation & Efficiency	AI enables automation, process optimization, and data-driven decisions – creating new duties for traceability and auditability.
Innovation & Competition	Data-driven services and generative models foster innovation but must comply with copyright and consumer-protection laws (cf. Art. 53 AI Act – transparency for GPAI).
Risks & Compliance	"Black-box" decisions entail liability and discrimination risks. The AI Act mandates fairness, explainability, and human oversight (Arts. 14–15).
Organization & Transformation	AI deployment requires governance structures, new roles (e.g., AI Compliance Officer, Data Steward), and AI literacy programs for employees (Art. 4 AI Act).

Typical Application Areas with Regulatory Relevance

- **Human Resources (HR):** Screening tools and chatbots → risk of algorithmic discrimination → high-risk under Annex III (2).
- **Finance:** Credit-scoring and fraud detection → high-risk under Annex III (5).
- **Marketing:** Profiling and targeting → transparency and information duties (Art. 52).
- **Industry:** Predictive maintenance → safety and reliability requirements (Art. 15).
- **Public Administration:** AI-supported application review → fundamental-rights assessment and FRIA requirement (Art. 27).

1.1.3 Historical and Legal Context

AI evolved from rule-based and expert systems of the 1980s toward machine learning and today's deep learning.
With increasing data availability and computational power, new societal and ethical questions have emerged.
The EU AI Act is the regulatory response: it extends the key principles of the GDPR – transparency, accountability, and responsibility – to AI systems.

1.1.4 Relevance for Governance and Compliance

AI is strategically critical and regulatorily demanding.
Organizations deploying AI must combine technological innovation with legal due diligence.

© A4Q Copyright 2025

The EU AI Act makes governance, risk management, and documentation a mandatory leadership responsibility.

Organizations are required to:

- Identify and manage risks systematically (Art. 9).
- Ensure data quality and fairness (Art. 10).
- Provide human oversight (Art. 14).
- Maintain an appropriate quality and management system (Arts. 17–23, ISO/IEC 42001).

1.2 Overview of the EU AI Act

The EU AI Act is part of the European Digital Rulebook and complements existing laws such as the GDPR, product safety and liability directives, and sectoral regulations (e.g., MDR, financial regulation, E-Commerce Directive).
Its objective is to create a trustworthy AI ecosystem that fosters innovation while protecting fundamental rights.

1.2.1 Key Principles of the AI Act

The EU AI Act establishes a set of core principles that form the foundation of trustworthy and lawful AI deployment across the European Union.
These principles ensure that AI systems are developed, tested, and used in a manner that protects safety, fundamental rights, and transparency while promoting innovation.
They define how organizations must structure their compliance, risk management, and governance processes throughout the entire AI lifecycle.

- **Risk-Based Approach (Art. 6 ff.)** – Classification of AI systems by risk and intended use.
  Transparency & Traceability (Arts. 13–15) – Obligation to disclose and document AI systems in a clear and understandable manner.
- **Human Oversight & Safety (Arts. 14–15)** – Prevention of fully autonomous decisions without human control.
- **Data Quality & Governance (Art. 10)** – Requirements for training and validation data.
- **Post-Market Monitoring & Corrective Actions (Arts. 61 ff.)** – Obligations after placing AI systems on the market.

© A4Q Copyright 2025

1.2.2 Roles and Responsibilities of Actors

The EU AI Act defines specific roles and responsibilities for all parties involved in the development, distribution, and use of AI systems.

These clearly assigned obligations ensure transparency, accountability, and consistent compliance across the entire AI supply chain – from development to market deployment and post-market monitoring.

Role	Core Responsibilities
Provider (Developer / Manufacturer)	Develops or places AI systems on the market; responsible for risk management, technical documentation, CE marking, and registration in the EU database.
Deployer (User / Operator)	Uses AI systems under its own responsibility; must ensure that systems are operated and monitored in accordance with the instructions for use.
Importer	Imports AI systems from third countries into the EU; verifies CE marking and conformity with EU requirements.
Distributor (Reseller)	Distributes AI systems within the EU; monitors markings and informs authorities about any deficiencies or non-conformities.
Authorized Representative	Acts on behalf of a provider established outside the EU and serves as the point of contact for market surveillance authorities.

1.3 Implementation Timeline (2024 – 2027)

The implementation of the EU AI Act follows a phased schedule to allow organizations, authorities, and market participants to gradually adapt to the new regulatory framework and compliance obligations.

Date	Entry into Force / Obligations
01 Aug 2024	Regulation (EU) 2024/1689 enters into force.
02 Feb 2025	Prohibited practices (Art. 5) and AI literacy obligations (Art. 4) become applicable.
02 Aug 2025	Obligations for General-Purpose AI Models (GPAI) (Arts. 53–55).
02 Aug 2026 – 2027	High-risk system obligations (Arts. 9–51) and conformity assessment procedures are fully applicable; market surveillance authorities are operational.

(Source: Art. 113 EU AI Act – Application and Transitional Provisions)

© A4Q Copyright 2025

1.4 Key Statement

The EU AI Act requires organizations to design, operate, and document the use of AI systems in a proactive, controlled, and transparent manner.

AI systems must, in the future, be not only technically safe but also legally verifiable.

This transforms AI compliance from an optional safeguard into a strategic component of responsible corporate governance.

© A4Q Copyright 2025

2 Risk-Based Approach & Classification

⏱ **Instruction time:** 60 minutes

🎯 **Business Outcomes:**

- **BO 2.1:** Participants acquire the competence to classify AI systems according to the four risk levels and derive the corresponding regulatory obligations.
- **BO 2.2:** Participants are prepared to plan appropriate measures and set priorities based on the degree of risk in order to allocate compliance resources effectively.

Learning Objectives (LO)

- **LO 2.1 (K1):** Participants know the four risk levels defined in the EU AI Act (unacceptable, high, limited, minimal) and understand their fundamental relevance for market access.
- **LO 2.2 (K2):** Participants can assign AI systems to the respective risk levels based on typical use cases and justify this classification.
- **LO 2.3 (K2):** Participants explain which regulatory obligations and documentation requirements arise from each risk level.
- **LO 2.4 (K3):** Participants can prioritize appropriate organizational and technical measures based on the risk classification and plan their implementation.
- **LO 2.5 (K3):** Participants can identify and evaluate transitions or changes in risk category and design suitable re-assessment processes.
- **LO 2.6 (K1):** Participants understand the relationship between risk classification, conformity assessment, and the resulting compliance obligations.

Key Terms:
Risk level, unacceptable risk, high risk, limited risk, minimal risk, Annex III, proportionality, risk dynamics, re-assessment, human oversight, AI risk review, risk prioritization, conformity assessment.

Introduction

This chapter explains the risk-based approach of the EU AI Act and describes how AI systems are classified according to their potential impact on safety, fundamental rights, and society. Participants understand why distinguishing between prohibited, high-risk, limited-risk, and minimal-risk categories is essential for determining regulatory obligations. It provides a foundation for understanding how risk assessment and compliance interact in practice.

© A4Q Copyright 2025

2.1 Fundamental Principle of the Risk-Based Approach

The EU AI Act follows the principle of proportionality: the higher the potential risk to fundamental rights, health, or safety, the stricter the corresponding obligations.
The level of risk, therefore, determines the overall compliance effort and the prioritization of internal measures.

Risk Level	Characteristics	Examples	Legal Consequences
Unacceptable Risk	Violation of human dignity or fundamental rights → Art. 5 AI Act	Social scoring, subliminal manipulation, and real-time biometric identification in public spaces	**Prohibited – market access not permitted**
High Risk	Decisions with material effects on individuals (Annex III)	Recruitment tools, credit scoring, medical AI	**Permitted only after full conformity assessment and CE marking**
Limited Risk	Human interaction, informational or deception risk	Chatbots, emotion recognition, deepfakes	**Permitted with transparency and labeling obligations**
Minimal Risk	No relevance for fundamental rights; everyday assistive systems	Spam filters, product recommendations	**Freely usable, no obligations – voluntary ethical standards recommended**

2.2 Annex III – Automatically High-Risk AI Systems

Annex III of the EU AI Act defines eight application areas whose purpose and context of use are considered particularly sensitive for society.
AI systems used for these specific purposes are classified as **high-risk**, regardless of their underlying technology or design.
What matters is not *how* the AI works technically, but *what it is used for* – that is, the intended purpose.

Definition of Purpose According to the EU AI Act

A system falls under Annex III if it:

© A4Q Copyright 2025

- makes decisions or assessments about individuals,
  affects fundamental rights, education, employment, safety, or the rule of law, or
  controls access to essential social or economic resources.

High-Risk Categories Under Annex III with Practical Examples

No.	Sector	Purpose of Regulation	Practical Example	Classification
1	Biometric identification and categorization	Protection against surveillance, profiling, and discrimination; limiting the use of sensitive biometric technologies.	A train station uses AI-based facial recognition to identify individuals on watchlists in real time.	High risk, partly prohibited under Art. 5
2	Critical infrastructure	Ensuring public safety and supply, AI failures must not cause physical harm.	An energy utility uses an AI system to automatically balance grid loads and prevent blackouts.	High risk, as malfunctions could endanger human safety
3	Education and vocational training	Ensuring fair and objective evaluation of learners; preventing algorithmic discrimination.	An e-learning platform analyzes essays and automatically assigns grades or feedback used in performance evaluation.	High risk (Annex III No. 3)
4	Employment, workforce management, and access to employment	Preventing discrimination in the workplace and ensuring transparent recruitment processes.	An HR system automatically screens job applications and creates ranked candidate lists for recruiters.	High risk
5	Access to essential private and public services	Safeguarding economic and social participation; ensuring fair decisions on credit, insurance, or social benefits.	A bank uses AI-based credit scoring to automatically approve or reject loan applications.	High risk, Art. 6 in conjunction with Annex III No. 5
6	Law enforcement and policing	Upholding due process and avoiding biased or erroneous prosecution.	Investigation software assesses the risk of reoffending and supports detention decisions.	High risk, subject to supervisory control

© A4Q Copyright 2025

No.	Sector	Purpose of Regulation	Practical Example	Classification
7	Migration, asylum, and border control	Protecting the fundamental rights of migrants; ensuring objective and rights-based procedures.	An AI-supported border-control system analyzes speech, gestures, and facial expressions of travelers to assess risk indicators.	High risk, with particular ethical sensitivity
8	Justice and democratic processes	Preserving judicial independence and the integrity of democratic decision-making.	A court uses AI-based decision-support software that analyzes past rulings to suggest sentencing outcomes.	High risk, Art. 6 in conjunction with Annex III No. 8

Example: Education and Vocational Training – Purpose and Delimitation

The purpose of Annex III No. 3 is to protect fairness and equal opportunity in the evaluation or advancement of learners.

Accordingly:

Use Case	Purpose Relevance	Classification
AI assesses learning performance, exams, or admissions	Directly influences educational opportunities	High risk
AI supports learners through feedback or adaptive learning pathways	Indirectly influences learning progression	High risk
Teachers use generative AI to prepare lessons or exam materials	No direct impact on learners, purely a preparatory purpose	Limited risk (Art. 52)
Writing or translation assistants used in class	Support function only, not for assessment purposes	Limited risk

Interpretation Note

Teachers who use AI solely to create or improve teaching materials, slides, or exercises are *not* operating a high-risk system.

Only when AI is used to assess learner performance or to influence learning processes directly is the application classified as high risk.

© A4Q Copyright 2025

Consequence

Systems with a purpose listed in Annex III are automatically classified as **high-risk AI systems** and are subject to the obligations set out in Arts. 9–24 EU AI Act, including in particular:

• Implementation of a risk-management system (Art. 9)
• Assurance of data quality and non-discrimination (Art. 10)
• Comprehensive technical documentation (Art. 11)
• Transparency and human oversight obligations (Arts. 13–14)
• Conformity assessment and CE marking (Arts. 17–23)

A later **change of purpose** (e.g., using a generative tool to perform automated grading) requires a new evaluation and, if applicable, re-classification to a higher risk level (Art. 6 (3)).

2.3 Criteria for Risk Classification

Even if a system is not listed in Annex III, providers and, where applicable, deployers must independently assess what risks may arise to health, safety, or fundamental rights in light of the system's intended purpose and operational context.
This assessment determines whether additional obligations under the EU AI Act apply (e.g., risk management, documentation, human oversight).

Applying the Risk Criteria

The following five criteria help to determine the risk level in a transparently and consistently.
They must be considered **in combination** – no single criterion alone determines the outcome.
The more criteria are answered with "yes," the more likely the system falls into a higher risk category (high/limited risk).

Criterion	Guiding Question	Meaning in Practice	Typical Consequence
1. Purpose & Impact	Does the system make decisions that affect individuals (e.g., selection, evaluation, access)?	AI that makes decisions about people or their rights is considered particularly sensitive.	Fundamental rights and ethics review required.
2. Operational Context	Is the AI used in safety-critical or public environments (e.g., healthcare, public administration, education)?	The more public or safety-relevant the context, the higher the potential risk for third parties.	May trigger additional oversight, notification, or reporting duties by national competent authorities.

© A4Q Copyright 2025

Criterion	Guiding Question	Meaning in Practice	Typical Consequence
3. Degree of Autonomy	Can the system act or decide independently without human approval?	Errors may be difficult to correct; human intervention must be possible.	If classified as high risk, human oversight obligations apply in accordance with Art. 14 EU AI Act.
4. Affected Group	Does the system involve vulnerable persons (children, patients, employees, migrants)?	These groups enjoy heightened legal protection.	Increased due diligence and monitoring obligations.
5. Scale of Impact	How many people are potentially affected or influenced?	Systems with a broad user base raise collective-risk concerns (e.g., social scoring).	More extensive documentation and evidence requirements.

Assessment Logic (Risk Profile)

Evaluation Result	Interpretation	Typical Classification
0–1 criteria apply	No significant impact on individuals or rights	→ Minimal risk (e.g., spell-checking AI, spam filters)
2–3 criteria apply	Potential influence on perception or information	→ Limited risk (e.g., chatbots, learning-support AI)
4–5 criteria apply	Impact on fundamental rights, safety, or living conditions	→ High risk (e.g., candidate selection, credit scoring)

Practical Guidance for Application

1. **Define the purpose:** What concrete goal does the AI application pursue (e.g., inform, evaluate, control)?
2. **Understand the context:** In what environment and with which users or stakeholders is it deployed?
3. **Check autonomy:** Is there human control, or does the system act autonomously?
4. **Analyze consequences:** What happens if the AI makes a mistake – who would be affected?

© A4Q Copyright 2025

5. **Document decisions:** The chosen risk level must be justified and traceable (e.g., in the *AI Risk Register* or Annex IX documentation).

No Fixed Scoring Model Under the EU AI Act

The EU AI Act does **not** provide a numeric or algorithmic scoring matrix.
According to Art. 6 (2)–(3), the assessment must consider qualitative factors when a system is not automatically classified as high-risk via Annex III:

"… taking into account the intended purpose, the output, and the impact of the system on the rights or safety of persons …"

This means:

- There are no fixed thresholds or point values.
- Each evaluation depends on context.
- This openness is deliberate – rigid metrics would hinder innovation.
- The result: risk classification is **interpretive** – "rule-guided but not rule-determined" – a consciously legal-ethical design intended to promote responsibility rather than automation.

How Greater Precision Will Be Achieved: "Guidance" and "Harmonized Standards"

Because the law itself remains open-ended, more detailed guidance will follow from supplementary instruments:

Source	Role	Status (October 2025)
AI Office / AI Board	Develops *Guidelines for Risk Classification* (common criteria for authorities and organizations)	Draft in progress; publication Q1 2026
CEN / CENELEC JTC 21	Prepares harmonized European standards (e.g., EN ISO/IEC 42001, 23894, and draft ISO/IEC TR 42006 on AI Compliance Frameworks)	Partially published
European Commission (Delegated Acts)	May later designate or downgrade certain systems as high-risk	Ongoing under Art. 7 EU AI Act

A more structured and harmonized assessment process will therefore become possible once these complementary guidance documents and delegated acts are formally adopted by the European

© A4Q Copyright 2025

Commission.
Until then, organizations must **document transparently** how they reached their conclusions.

Why This Openness Is Intentional – and Where the Limits Lie

This openness is **not a flaw** but part of the governance concept.

The AI Act is designed to make organizations:

Identify, justify, and document risks, instead of relying on rigid numerical thresholds.

However, the assessment must not be arbitrary – it must be **reasoned, consistent, and auditable**, for example, by:

- Providing written justification (e.g., in the *AI Risk Register*),
- Referring to official definitions (Arts. 3 and 6, Annex III),
- Using harmonized standards (ISO/IEC 23894 as reference framework).

In conformity assessments or regulatory audits under Arts. 43–51, the emphasis lies not on numeric scores but on the documented justification and traceability of the chosen risk classification.

Conclusion

Risk classification is not a technical calculation but a **legal and ethical assessment** of an AI system's intended purpose.
The more an AI system influences human decisions or fundamental rights, the higher its risk level – and the more comprehensive its compliance obligations.

2.4 Obligations and Measures by Risk Level

The obligations of an organization depend directly on the risk level of the AI system.
The higher the potential risk to individuals, fundamental rights, or safety, the stricter the legal requirements.
The following overview summarizes the four levels, their legal basis, typical obligations, and recommended implementation measures within an organization.

Overview: Risk Levels, Legal Obligations, and Organizational Measures

© A4Q Copyright 2025

Risk Level	Legal Basis & Key Obligations	Practical Meaning	Typical Organizational Measures
🟥 **Unacceptable Risk**	Art. 5 EU AI Act – Prohibition of certain practices: • Subliminal manipulation (unconscious influence) • Exploitation of vulnerabilities (e.g., children, patients) • Social scoring by public authorities • Real-time biometric surveillance in public spaces	These systems must **not** be developed, marketed, or deployed. If identified, they must be immediately stopped and reported to the competent authority.	– Internal stop procedure when a prohibited practice is suspected – Immediate deactivation and data preservation – Notification to compliance / supervisory authority (incident report) – Ethics review: root-cause analysis and prevention plan
🟧 **High Risk**	Arts. 6–51 EU AI Act – Comprehensive obligations: • Risk-management system (Art. 9) • Data and data-quality requirements (Art. 10) • Technical documentation (Art. 11) • Transparency and user information (Art. 13) • Human oversight (Art. 14) • Accuracy, robustness, and cybersecurity (Art. 15) • CE marking and EU declaration of conformity (Art. 49)	High-risk systems may only be placed on the market or used after a successful conformity assessment. They must remain verifiable and traceable at all times.	– Implement an AI risk-management system (e.g., per ISO/IEC 23894) – Maintain an AI Risk Register for all deployed systems – Document training data, models, and test results – Define human oversight procedures (who can intervene and how) – Conduct regular audits and retain CE conformity evidence – Train staff on compliance duties and incident reporting

© A4Q Copyright 2025

Risk Level	Legal Basis & Key Obligations	Practical Meaning	Typical Organizational Measures
🟧 **Limited Risk**	Art. 52 EU AI Act – Transparency obligations: • Users must be able to recognize AI interaction • Deepfakes, chatbots, emotion recognition, and generative content must be clearly labeled • For deepfakes: disclosure of manipulation or fictional nature	These systems are permitted but must disclose that AI is involved. The goal is to prevent deception and misinformation.	– User-interface notice (e.g., “Response generated by AI”) – Content labeling (watermarks or metadata) – Transparency page or FAQ describing AI usage – Internal review to ensure users are adequately informed – Provide opt-out options (e.g., for chatbots)
🟩 **Minimal Risk**	No direct AI Act obligations; voluntary alignment with standards: • Recitals 81–84 EU AI Act • ISO/IEC 42001 (AI Management System) • OECD and UNESCO Ethics Guidelines	These systems carry no regulatory duties because they pose no significant risk to rights or safety (e.g., spam filters, UI assistants). However, voluntary AI governance is recommended to demonstrate accountability.	– Establish an AI governance policy (e.g., internal ethics charter) – Publish a transparency statement on the company website (“We use AI in a supporting manner …”) – Document responsibilities (who reviews and approves AI use) – Perform a self-assessment based on ISO/IEC 42001-Light (simplified implementation)

© A4Q Copyright 2025

Explanation of the Levels in the Corporate Context

🟥 **Unacceptable – "Do not operate, do not sell, do not use"**

- These systems are **explicitly prohibited by law**.
- Organizations must ensure that no prohibited functionality forms part of any product or service.
- If a violation is detected, there is a **reporting obligation** and a risk of **severe administrative fines** (up to EUR 35 million or 7 % of annual turnover).

🟧 **High Risk – "Permitted, but only under strict control"**

- This category represents the core regulatory scope of the EU AI Act.
- The entire development and deployment process must be demonstrably safe, transparent, and controllable.
- Every high-risk system requires a technical file and CE marking before it can be used.
- In practice, this primarily applies to AI used in healthcare, education, HR, finance, security, and justice.

🟨 **Limited Risk – "Transparency obligation instead of audit requirement"**

- Systems in this category may be freely used but must clearly disclose AI involvement.
- • The focus is not on algorithmic control but on protecting users from deception or manipulation.
- • Particularly relevant for chatbots, generative AI, emotion recognition, and deepfakes.

🟩 **Minimal Risk – "Good practice rather than regulation"**

- These systems fall below the regulatory threshold of the AI Act.
- Lawmakers encourage voluntary ethical standards to foster trust and transparency.
- Even without legal obligations, documented self-commitments signal **audit readiness** and responsible AI governance.

Examples of Corporate Implementation

AI Application Type	Expected Risk Level	Obligations & Measures
Applicant-screening AI	High risk	CE marking, data-quality controls, human oversight
Customer-service chatbot	Limited risk	"You are chatting with an AI" notice, logging

© A4Q Copyright 2025

AI Application Type	Expected Risk Level	Obligations & Measures
Learning-support assistant	Limited risk	Transparency notice, content quality review
Facial-recognition system in public space	Unacceptable risk	Prohibited use, internal incident report
Text-summarization tool for teachers	Minimal risk	Voluntary AI governance, internal review

Conclusion

The **risk level determines the applicable obligations**.
The AI Act does not aim to ban technology but to ensure **accountability and proportionality**.
Organizations must therefore:

- Document the justified risk level for every AI system.
- Actively implement the corresponding obligations and measures.
- Re-evaluate and update the classification whenever the system's purpose or functionality changes.

2.5 Risk Dynamics and Re-Assessments

AI systems may change their risk level over their lifecycle – for example, due to new functionalities, updates, or a change of intended purpose.
Organizations must therefore implement structured processes for **regular reassessments** to ensure continuous compliance with the EU AI Act.

Trigger	Possible Consequence	Required Action
Functional expansion → new decision logic	Limited → High risk	Conduct a new conformity assessment in accordance with Arts. 17–23 EU AI Act
Use in a critical domain (e.g., healthcare)	Minimal → High risk	Perform an AI risk review and notify the competent authority
Automation without human oversight	High → Potentially unacceptable	System shutdown and renewed evaluation

© A4Q Copyright 2025

2.6 Risk-Based Prioritization of Measures

The risk level not only determines regulatory obligations but also defines **the internal priority of compliance activities**.
A structured prioritization approach allows organizations to allocate resources efficiently based on risk severity.

Priority Level	**Typical Areas**	**Recommended Measures**
1 (High Risk)	HR, finance, healthcare, justice	Formal risk management, internal and external audits, CE conformity process
2 (Limited Risk)	Marketing, communications, generative AI	Labeling, transparency reporting
3 (Minimal Risk)	Internal support systems, process automation	Voluntary ethics checks, staff awareness training

→ Risk-based prioritization enables the efficient use of limited compliance resources and helps focus governance efforts where they matter most.

© A4Q Copyright 2025

3 Global and Sectoral Regulatory Landscape (Overview)

⏱ **Instruction time:** 70 minutes

🎯 **Business Outcomes (BOs)**

- **BO 3.1:** Participants develop an in-depth understanding of international AI regulations and are able to critically assess their application in global projects.
- **BO 3.2:** Participants can identify opportunities for harmonization between EU and non-EU regulatory frameworks and strategically leverage them within their organization.

Learning Objectives (LOs)

- **LO 3.1 (K2):** Participants can describe and distinguish between major current AI regulatory approaches (e.g., EU, United States, China, United Kingdom, Canada, Brazil, OECD, United Nations, Council of Europe).
- **LO 3.2 (K3):** Participants can interpret recent developments—such as China's labeling requirements for AI-generated content effective September 1, 2025—within the context of global AI governance and apply them through a practical example.
- **LO 3.3 (K3):** Participants can explain and compare key similarities and differences between the EU AI Act and other international frameworks.
- **LO 3.4 (K3):** Participants can identify core opportunities for harmonization in multinational projects and illustrate practical integration approaches.
- **LO 3.5 (K2):** Participants can explain sector-specific regulatory regimes (e.g., healthcare, finance, automotive, defense) and their relationship to AI regulation.
- **LO 3.6 (K1):** Participants understand the relevance of international cooperation and multilateral bodies (e.g., OECD, G7, UN, Council of Europe) for advancing and aligning AI regulation worldwide.

Key Terms:
OECD AI Principles, UNESCO Recommendation on AI Ethics, NIST AI RMF, G7 Code of Conduct, Council of Europe CAI, AI Safety Summit, US Executive Order on AI, China Generative AI Regulation, AI Liability Directive, Data Act, Cyber Resilience Act (CRA), Digital Services Act (DSA), GDPR, Data Protection Impact Assessment (DPIA/DSFA).

© A4Q Copyright 2025

Introduction

This chapter provides an overview of the international and sector-specific regulatory landscape for artificial intelligence. It outlines how different regions – including the European Union, the United States, the United Kingdom, China, and others – are developing distinct yet increasingly aligned approaches to AI governance. Participants gain an understanding of how global frameworks, guidelines, and industry standards contribute to the harmonization of AI governance and compliance practices.

3.1 Global AI Regulation: Status and Trends

European Union (EU)

The EU Artificial Intelligence Act is internationally regarded as one of the most comprehensive and binding legal frameworks for AI.

With the implementation of the **GPAI rules for foundation models** in 2025, pressure on major providers of generative AI systems has increased significantly.

Core elements such as **transparency obligations**, **risk management**, and **CE conformity** are effectively setting **global benchmarks** for exports and international competition.

China (Regulatory Status as of September 2025)

Since **August 15, 2023**, the *Interim Measures for the Management of Generative AI Services* have been in effect.

These require public providers of generative AI services to ensure **content moderation**, **data quality**, **algorithmic transparency**, and **user complaint mechanisms**.

Effective **September 1, 2025**, the new *Labeling Rules for AI-Generated Content* come into force.

They require providers to apply both **visible user-facing labels** and **invisible metadata tags** to text, image, audio, video, and 3D content generated by AI systems.

Digital platforms (e.g., social-media networks) must automatically detect, classify ("confirmed / possible / suspected AI-generated"), and, where necessary, relabel AI-produced content.

Starting **November 1, 2025**, national technical standards will define label and metadata formats as well as security requirements for data annotation, training, and fine-tuning processes.

In parallel, China released its *Global AI Governance Action Plan 2025*, aimed at expanding its influence on international AI standardization and norm-setting.

Implications for international projects:

Companies that produce or distribute content for the Chinese market must implement the mandatory **AI labeling (labels + metadata)** requirements starting in September 2025.

These obligations are technically specific and demand adaptations of existing **content and publishing**

© A4Q Copyright 2025

pipelines.
China's regulatory approach is modular and highly responsive to emerging technologies (e.g., deep synthesis, recommendation algorithms).
The global governance plan underscores China's ambition to position its AI standards as international reference points – both as a contribution to harmonization and as a tool of **geopolitical influence**.

United States (US)
The United States currently has **no single federal AI law**.
Regulation is **sector-specific and decentralized**, primarily through:
• the **NIST AI Risk Management Framework (2023)** as a voluntary standard,
• various **Executive Orders** and policy strategies (e.g., the *Blueprint for an AI Bill of Rights*), and
• **state-level initiatives** (e.g., California) introducing transparency and accountability requirements.
The focus lies on **self-regulation, responsibility, and governance-based risk management**.

United Kingdom (UK)
The UK continues to pursue a **principles-based, pro-innovation approach**.
Rather than enacting a single AI law, the government updates existing legislation and issues cross-sector guidance focused on **transparency, fairness, and safety**.

Canada
The proposed **Artificial Intelligence and Data Act (AIDA)** introduces binding requirements for **risk and impact assessments**, **accountability measures**, and **audits**.
The legislative proposal is closely aligned with the **European model** and is expected to become particularly relevant for international providers active in the Canadian market.

Brazil and Latin America
Brazil is developing its **Marco Legal da Inteligência Artificial** (draft 2024), a framework emphasizing **risk-based regulation, transparency, and ethics**.
Other countries in the region are increasingly adopting regulatory approaches inspired by the EU system.

International Organizations and Soft Law
The **OECD AI Principles (2019)**, the **UNESCO Recommendation on AI Ethics (2021)**, and the **Council of Europe's draft AI Convention** form the foundation for a global dialogue on AI governance.
These **soft-law instruments** promote alignment and cooperation among countries that have not yet implemented binding AI legislation.

© A4Q Copyright 2025

3.2 Comparison: EU AI Act ↔ International Regulations

The following comparison outlines how the EU AI Act differs from and aligns with major international regulatory frameworks.
It highlights varying legal approaches, enforcement mechanisms, and transparency requirements, while illustrating the emerging trend toward risk-based convergence across jurisdictions.

Aspect	**EU AI Act**	**China (Labeling from Sept 2025)**	**United States / NIST Framework**	**Canada (AIDA Draft)**	**United Kingdom / Principles-Based Approach**
Legal Nature	Regulation – binding and directly applicable within the EU	Administrative regulation / technical directive	Voluntary framework / guidance	Legislative proposal	Principles-based guidance
Risk-Based Approach	Four levels: prohibited – high – limited – minimal	Tiered supervision without formal risk classes	Process-oriented risk evaluation	Modeled after the EU approach	No formal classification
Transparency / Labeling	Mandatory disclosure and labeling (Arts. 52 ff.)	As of Sept 1 2025: visible and invisible labels for all AI-generated content	Transparency recommended	Reporting obligations under development	Transparency encouraged, not mandatory
Audit / Conformity	External conformity assessment + CE marking	Algorithm filing + security inspections	Self-assessment or third-party review	External reviews envisaged	Accountability is encouraged but optional
Sanctions	Fines up to €30 million or 6 % of annual turnover	License revocation, monetary fines, blacklisting	No centralized sanctions	Administrative fines planned	Low enforceability

© A4Q Copyright 2025

Note:
China's new labeling regulation (effective September 2025) complements its existing generative-AI measures and, for the first time, establishes precise **technical labeling and metadata requirements**. Many non-European frameworks (e.g., Canada, Brazil) are **aligned with the EU's risk-based logic**, facilitating global harmonization – provided that regional security and data-governance requirements are respected.

3.3 Sectoral AI Regulation and Interfaces

AI regulation increasingly intersects with sector-specific frameworks that impose additional safety, accountability, and ethical requirements.
The table below summarizes key sectors where AI-specific provisions or standards apply and illustrates how these intersect with broader AI governance obligations.

Sector	Relevant Regulations	Key AI Requirements
Healthcare / MedTech	EU MDR / IVDR, FDA AI/ML Guidance (US)	Safety, validation of training data, bias control, and clinical evidence
Finance / Insurance	Basel Committee, EBA Guidelines, SEC / FINRA (US)	Algorithmic fairness, auditability, risk management
Automotive / Mobility	UNECE WP.29, ISO 26262, ISO 21448 (SOTIF)	Safety-by-design, real-time monitoring, redundancy
Defense / Security	UN CCW, EU Dual-Use Regulation 2021/821	Civil-military distinction, export control
Education / EdTech	UNESCO AI in Education (2023)	Protection of minors, data ethics, and transparency

3.4 Harmonization and Strategies for Global AI Projects

To ensure effective and consistent implementation of international AI compliance, globally operating organizations can adopt the following **strategic and organizational approaches**:

© A4Q Copyright 2025

(1) "Baseline + Local Add-On"

• Build a **central AI compliance framework** based on the EU AI Act and ISO/IEC 42001.

• Supplement it with **country-specific modules** (e.g., Chinese labeling obligations, U.S. guidelines, Canadian AIDA requirements).

• Use **modular policies** and **region-specific compliance profiles** to enable flexibility across jurisdictions.

(2) Standards and "Presumption of Conformity"

• Align early with **ISO/IEC 42001**, **ISO/IEC 23894**, **ISO/IEC 27001**, and relevant **IEEE guidelines**.

• Unified standards facilitate the **demonstration of conformity** outside the EU and strengthen cross-border trust.

(3) "Regulation Tracking & Gap Mapping"

• Continuously monitor global regulatory developments (e.g., China, U.S., Latin America, and others).

• Create **cross-reference mappings** (e.g., EU labeling ↔ Chinese labeling).

• Conduct regular **gap analyses** to identify priorities and define compliance roadmaps.

(4) Global Governance Structures

• Establish an **AI Governance Board** with regional compliance representatives.

• Define **clear escalation, coordination, and reporting channels** between global and local entities.

(5) Content-Pipeline Architecture and Modularity

• Develop **content pipelines** integrating automatic labeling and regional compliance validation.

• Enable **dynamic switching to country-specific policies** (e.g., for content published in China).

• Ensure **version control, logging, and auditability** for all releases.

Example:

A company operates a **global content platform** serving the EU, China, and North America.
Its core governance model follows the **EU AI Act** and **ISO/IEC 42001**.
For the Chinese market, it integrates **automatic visible and metadata-based labels** in accordance with the obligations effective **September 1, 2025**.
The **AI Governance Board** continuously monitors new requirements and prioritizes the adaptation of technical and organizational processes.

3.5 Summary and Key Messages

• **Global AI regulation** is evolving dynamically. China will introduce **binding labeling obligations** in September 2025 that must be implemented with precise technical specifications.

• The **EU AI Act** currently represents the most stringent legal framework worldwide and shapes the global regulatory logic for trustworthy AI.

• **Soft-law instruments** such as the **OECD AI Principles** and the **UNESCO Recommendation on AI**

© A4Q Copyright 2025

Ethics promote convergence between jurisdictions.

• Organizations should develop a **modular compliance system** that reflects local specifics while maintaining a unified global governance structure.

• The long-term goal is to **leverage harmonization potential** through **standard alignment, labeling interoperability,** and **early identification of regulatory conflicts**.

© A4Q Copyright 2025

4 Prohibited AI Practices (Art. 5 EU AI Act)

⏱ **Instruction time:** 50 minutes

🎯 **Business Outcomes:**

- **BO 4.1:** Participants develop awareness of prohibited AI practices and can identify such practices within their organizational context.
- **BO 4.2:** Participants are prepared to assess and apply the exceptions outlined in Article 5 of the EU AI Act.

Learning Objectives (LOs)

- **LO 4.1 (K1):** Participants know the four main categories of prohibitions under Article 5 of the EU AI Act and understand their basic distinctions.
- **LO 4.2 (K2):** Participants can explain why certain AI practices are deemed prohibited and which fundamental rights they infringe upon.
- **LO 4.3 (K3):** Participants can identify examples of prohibited AI applications within their organizational or public-sector context and assess their potential legal consequences.
  LO 4.4 (K2): Participants can explain the conditions and limits of the exceptions set out in Articles 5(2) and 5(3).
- **LO 4.5 (K1):** Participants understand the legal consequences and possible types of sanctions for violations of Article 5 and their implications for AI compliance practice.

Key Terms:
Subliminal manipulation, behavioral steering, social scoring, biometric categorization, real-time biometrics, fundamental rights, human dignity, security interest, exception (Art. 5 (2)–(3)), market prohibition, legal consequences.

Introduction

Article 5 of the EU AI Act establishes a *"red line"* – certain types of AI applications are strictly prohibited for reasons of fundamental rights protection.
These prohibitions apply regardless of technical performance or economic value.
Their primary purpose is to safeguard human dignity, freedom of thought and expression, and individual autonomy.

© A4Q Copyright 2025

4.1 Overview of Prohibited Practices

According to Article 5(1) of the EU AI Act, the following AI practices are prohibited:

No.	Prohibited Practice	Description / Example	Protected Interest
1	**Subliminal manipulation**	Systems that steer human behavior below the threshold of conscious awareness (e.g., nudging via unnoticed stimulus patterns).	Autonomy, freedom of decision-making
2	**Exploitation of vulnerable groups**	AI systems that deliberately influence children, the elderly, or persons with disabilities (e.g., toys exploiting emotional attachment).	Protection of vulnerable persons
3	**Social scoring by public authorities**	Evaluation of citizens' behavior or character across multiple contexts (e.g., bonus or penalty systems for "desirable" behavior).	Equality, human dignity
4	**Real-time biometric identification in public spaces**	Facial recognition or other biometric systems used for public surveillance (e.g., crowd scanning in public areas).	Privacy, freedom of movement

These applications are strictly prohibited – they may not be developed, marketed, or deployed under any circumstances.

4.2 Legal and Fundamental Rights Basis

The prohibitions are grounded in the **Charter of Fundamental Rights of the European Union**, in particular:

- Article 1 – Human dignity
- Article 7 – Respect for private and family life
- Article 8 – Protection of personal data
- Article 21 – Non-discrimination

© A4Q Copyright 2025

The European Commission emphasizes that the AI Act sets not only **technical boundaries** but also **ethical limits**, aimed at preventing surveillance, manipulation, and social coercion through automated evaluation systems.

4.3 Exceptions under Article 5(2)–(3)

Under strict conditions, **real-time biometric identification in public spaces** may be permitted if it:
• is explicitly provided for by law,
• serves a narrowly defined purpose (e.g., investigation of serious crimes, counter-terrorism, or locating missing persons),
• is carried out by a competent public authority with **judicial authorization**, and
• is **limited in time and scope**.

The **burden of proof** regarding necessity and proportionality lies with the competent authority.
Private companies may not deploy such systems independently but only under **formal government authorization** and in accordance with **national implementing legislation**.

4.4 Practical Awareness Measures

To strengthen compliance culture, organizations should:

1. Maintain an **AI register** listing all active and planned AI applications.
2. Use **compliance checklists** to identify whether an AI application might fall into a prohibited category.
3. Conduct **ethical and legal reviews** before project initiation.
4. Offer **awareness and compliance training** for developers, product managers, and marketing teams to recognize manipulation or scoring mechanisms.

4.5 Practical Examples

Practical Examples Illustrating Prohibited AI Practices

The following examples demonstrate typical scenarios in which AI systems would violate the prohibitions established under **Article 5 of the EU AI Act**.
They are intended to raise awareness of potentially unlawful practices and to illustrate how technological innovation must be aligned with legal and ethical boundaries.

© A4Q Copyright 2025

1 Subliminal Manipulation

Example 1: Emotion-based advertisement optimization

An online advertising platform uses AI to analyze users' micro-expressions and heart-rate patterns via webcam to adapt colors, sounds, or text in real time – without the users' awareness.

→ This constitutes subliminal influence because it manipulates emotional states below the level of conscious perception.

Example 2: Neural-feedback gaming

A virtual-reality game detects players' brain-wave activity and adjusts difficulty and reward stimuli to increase playtime without explicit consent.

→ The system covertly alters behavior through subconscious conditioning and therefore infringes on autonomy and free will.

2 Exploitation of Vulnerable Groups

Example 1: AI-enabled companion toy for children

An interactive doll uses generative AI to build emotional attachment and encourage in-app purchases or data sharing.

→ Children's trust is intentionally exploited, violating protections for minors and ethical marketing standards.

Example 2: Elder-care monitoring assistant

An AI system in a care home manipulates elderly residents into taking medication or providing feedback through deceptive prompts.

→ It abuses cognitive or emotional vulnerability, undermining informed consent and dignity.

3 Social Scoring by Public Authorities

Example 1: Citizen behavior rating system

A municipality assigns citizens a "civic reliability score" based on payment history, social-media posts, and law-enforcement data to determine access to public services.

→ This cross-context evaluation discriminates and restricts participation, violating equality and human dignity.

Example 2: Public-benefit eligibility ranking

An AI tool aggregates employment, tax, and health records to rank applicants for welfare benefits.

→ It creates systemic bias and stigmatization, breaching the prohibition on automated social classification.

© A4Q Copyright 2025

4 Real-Time Biometric Identification in Public Spaces

Example 1: Crowd-scanning at transport hubs
A city police department deploys facial-recognition cameras in train stations to identify persons of interest in real time.
→ Such continuous biometric surveillance compromises privacy and freedom of movement unless authorized under narrowly defined exceptions.

Example 2: Emotion-detection at public events
AI-powered cameras at a concert analyze spectators' facial expressions to flag "agitated" individuals for security staff.
→ This represents unlawful biometric profiling and real-time behavioral monitoring without a legal basis.

Exceptions to the Prohibited AI Practices under Article 5 of the EU AI Act

The prohibitions defined in Article 5 of the EU AI Act are, in principle, absolute.
However, in narrowly defined exceptional cases, certain applications may be permitted if they are **legally authorized**, **proportionate**, **necessary**, and conducted under **human oversight**.
The following examples illustrate possible exceptions for each of the four categories of prohibited practices, highlighting the core principles of **proportionality** and **purpose limitation**.

1 Subliminal Manipulation – Exception

Example: *Public health awareness campaign using mild persuasive cues*
A public health authority deploys an AI-based digital poster that subtly changes color or background music to draw attention to vaccination information in public areas.
→ As long as the system does not manipulate individual decisions below the level of consciousness or exploit personal vulnerabilities, and the intention is **public interest communication**, it is not considered subliminal manipulation under Article 5.

2 Exploitation of Vulnerable Groups – Exception

Example: *Assistive AI technology for children or elderly users*
An AI-based reading assistant adapts language complexity and tone to support children or elderly persons in understanding official documents.
→ The system provides accessibility support rather than influence. When used **for empowerment and inclusion**, and not to steer behavior or extract data, it remains lawful.

3 Social Scoring by Public Authorities – Exception

© A4Q Copyright 2025

Example: *Administrative risk scoring for compliance or fraud prevention*
A tax authority uses AI to detect potentially fraudulent patterns in financial declarations. The scoring is **limited to a single administrative context**, with **human review and legal safeguards** in place.
→ Such risk-based models are allowed if they **do not evaluate moral or behavioral characteristics** across domains and are used solely to ensure legal compliance.

4 Real-Time Biometric Identification in Public Spaces – Exception (Article 5(2)–(3))

Example: *Police search for a missing child under judicial authorization*
Law enforcement uses a real-time facial recognition system at a train station to locate a missing minor.
→ The deployment is **legally authorized**, **judicially approved**, **limited in time and location**, and **proportionate** to the objective.
→ This represents one of the **explicit exceptions** foreseen under the EU AI Act.

These exceptions illustrate that **Article 5 prohibitions are absolute in principle**, yet **narrowly limited allowances** may exist when:

- the purpose serves a **legitimate public interest**,
- safeguards ensure **proportionality and necessity**, and
- **human oversight and legal authorization** are strictly maintained.

4.6 Summary

Chapter 4 defines the AI practices explicitly **prohibited under Article 5(1) EU AI Act**, which apply regardless of a system's technical capability or economic value. These include:
(1) *subliminal manipulation* (Art. 5 (1)(a)),
(2) *exploitation of vulnerable groups* (Art. 5 (1)(b)),
(3) *social scoring by public authorities* (Art. 5 (1)(c)), and
(4) *real-time biometric identification in public spaces* (Art. 5 (1)(d)).
Such systems are **strictly prohibited** from being developed, marketed, or used within the EU.
Exceptions under *Articles 5 (2)–(3)* apply only to narrowly defined law-enforcement purposes (e.g., searching for missing persons or preventing terrorism) when legally authorized, proportionate, time-limited, and subject to judicial oversight.

© A4Q Copyright 2025

5 High-Risk AI Systems and Obligations (Arts. 6–51 EU AI Act)

⏱ **Instruction Time:** 120 minutes

🎯 **Business Outcomes:**

- **BO 5.1:** Participants acquire the ability to identify the relevant obligations for high-risk AI systems, support their practical implementation within the organization, and contribute to compliance with legal requirements.
- **BO 5.2:** Participants are sensitized to create verifiable documentation and evidence to enhance audit readiness and regulatory assurance.

Learning Objectives (LOs)

- **LO 5.1 (K1):** Participants know the basic classification of AI systems as high-risk under Articles 6–7 of the EU AI Act and understand which types of applications fall within this category.
- **LO 5.2 (K2):** Participants can describe the core obligations for high-risk AI systems as outlined in Articles 6–51 of the EU AI Act.
- **LO 5.3 (K3):** Participants can design an operational approach for implementing the key compliance duties (risk management, data quality, human oversight, documentation).
- **LO 5.4 (K3):** Participants can prepare or assess audit-ready documentation and evidence for high-risk AI systems.
- **LO 5.5 (K1):** Participants know the main articles within the high-risk section (Arts. 9–15) and their fundamental purposes.

Key Terms:
High-risk AI, Articles 6–51 EU AI Act, Annex III categories, conformity assessment, CE marking, risk management system, human oversight, documentation requirement, data quality, technical robustness, bias control, audit trail, lifecycle, AI Quality Management System (AI QMS).

Introduction

High-risk AI systems represent the core regulatory focus of the EU AI Act. They are not prohibited, but their use is permitted only under strict legal and technical conditions. Articles 6 to 51 define a coherent set of obligations combining technical, organizational, and documentation requirements. The objective is to

© A4Q Copyright 2025

safeguard fundamental rights, safety, and fairness while maintaining space for innovation and competitiveness.

This chapter provides a practical, implementation-oriented overview of how organizations can comply with these legal obligations, fulfill documentation and evidence requirements, and establish audit readiness for high-risk AI systems.

5.1 Identification of High-Risk AI Systems

According to **Article 6** in conjunction with **Annex III** of the EU AI Act, an AI system is considered *high-risk* if it is used in one of the sensitive areas listed therein or forms part of a safety-related product already subject to an **EU conformity assessment** (e.g., medical devices, lifts, machinery, vehicles).

Domain	**Typical Example**	**Legal Basis / Reference**
Human Resources (HR)	Automated candidate screening, performance evaluation	Art. 6 in conjunction with Annex III No. 4
Credit and Finance	Credit scoring or creditworthiness assessment systems	Annex III No. 5
Education & Training	Automated exam grading, admission systems	Annex III No. 3
Healthcare	Diagnostic decision support, prioritization systems	Annex III No. 2
Criminal Justice & Security	Risk or recidivism prediction, evidence analysis	Annex III No. 6
Public Administration	Automated eligibility assessments, welfare decisions	Annex III No. 7

Criteria (Art. 6 EU AI Act)

A system is classified as high-risk if:

1. it is likely to have a significant impact on the fundamental rights or safety of individuals,
2. it makes decisions or recommendations in a regulated domain,
3. it operates automatically or semi-automatically, and

© A4Q Copyright 2025

4. its potential risks cannot be adequately mitigated through human oversight or transparency measures.

Practical Check for Organizations

- **Question 1:** Does the system make decisions with legal or economic consequences for individuals (e.g., rejection, access, pricing)?
- **Question 2:** Is the system deployed in a sector listed in **Annex III**?
- **Question 3:** Can the system generate outputs or actions **without human review**?
- **Question 4:** Is the system covered by an existing **regulatory framework** (e.g., medical device, vehicle safety, labor law)?

If **one or more questions** are answered "yes," a **high-risk classification** is highly probable, and a **formal conformity assessment procedure** under **Articles 16 ff.** may be required.

Recommended Organizational Practices

- Maintain a central AI register with information on purpose, risk classification, and the responsible person.
- Use a standardized screening form for risk identification (e.g., based on ISO/IEC 42001).
- Document the reasoning, references, and classification decision in the audit dossier.
- In case of uncertainty, consult legal or compliance departments or the national supervisory authority.

5.2 Core Obligations for High-Risk AI Systems

Articles 9–24 of the EU AI Act form the foundation of obligations for high-risk AI systems.
They define how providers and deployers must ensure that systems remain reliable, explainable, and under human control throughout their entire lifecycle.

The requirements include technical, organizational, and documentation-based measures – from data quality and risk management to post-market monitoring.
For organizations, this means that every high-risk AI system must be covered by an integrated compliance framework with clearly defined processes, responsibilities, and evidence.

The following overview outlines the key obligations, their legal basis, and typical implementation and audit measures in practice.

© A4Q Copyright 2025

Topic Area	Article(s)	Objective	Practical Implementation / Audit Evidence
Risk Management System	Art. 9	Systematic identification, evaluation, and mitigation of risks throughout the lifecycle	Establish an **AI Risk Register**, define assessment methods, perform regular re-evaluations upon system changes
Data Quality & Governance	Art. 10	Ensure high-quality, fair, and representative training, validation, and test data	Document data sources, perform **bias analyses**, track **fairness metrics**, and maintain **data steward approval logs**
Technical Documentation	Art. 11	Ensure full traceability and accountability toward authorities	Create a **technical dossier** (system description, models, data, risks, test results), versioning, and secure archiving
Logging & Audit Trail	Art. 12	Guarantee traceability and evidence for every system decision	Implement tamper-proof **logs** (timestamp, input/output, user ID), with **hashing** or **WORM storage**
Transparency & User Information	Art. 13	Provide clear information about purpose, functionality, limitations, and risks	Use **standardized user notices**, an **explainability layer**, and internal **guidance documents**
Human Oversight	Art. 14	Ensure effective human control and intervention capability	Define **roles and approval workflows**, implement **human-in-the-loop mechanisms**, and train authorized staff
Robustness, Accuracy & Cybersecurity	Art. 15	Guarantee system reliability under errors or attacks	Conduct **stress tests**, **adversarial testing**, **vulnerability scans**, and establish **backup/recovery procedures**
Conformity Assessment & CE Marking	Arts. 16–23	Demonstrate compliance prior to market placement	Perform internal or external **conformity assessments**, issue **EU Declaration of Conformity**, apply **CE marking**, and register in the **EU AI Database**

© A4Q Copyright 2025

Topic Area	Article(s)	Objective	Practical Implementation / Audit Evidence
Post-Market Monitoring & Incident Reporting	Art. 24 ff.	Monitor performance and ensure continuous improvement after market placement	Implement **monitoring plans**, an **incident response process**, periodic **audit reports**, and a **feedback loop** to risk management
Change Management & Revalidation	Art. 43(2), 61	Ensure reassessment after substantial modifications	Establish a **change-control process**, document model updates, and reanalyze risks after retraining or purpose changes
Documentation & Audit Readiness	Arts. 11, 61	Provide verifiable evidence for all obligations	Maintain a unified **audit repository**, checklists, training records, and a **traceability chain** “from data to decision”

5.3 Implementation within Organizations

The practical implementation of high-risk AI obligations requires coordinated collaboration between technical teams, compliance functions, and business units.
The objective is to establish a verifiable process that identifies risks, ensures traceable decision-making, and maintains audit readiness.

1 Risk Management (Art. 9 EU AI Act)

• Establish an **AI Risk Register** with a unique system ID, defined purpose, and designated responsible person (“Owner per Use Case”).
• Assess all risks based on **likelihood × severity**, including bias, erroneous decisions, and misuse scenarios.
• Define **thresholds and escalation paths** (e.g., “critical > 0.6”).
• Conduct **periodic re-evaluations** after model updates, data changes, or deployment in new contexts.
• Document results in a **Risk Report**, forming part of the technical documentation.

2 Documentation (Arts. 11 and 17 EU AI Act)

• **Mandatory contents:** purpose, functionality, model description, data basis, testing and validation protocols, limitations, and known risks.

© A4Q Copyright 2025

• **Version control:** every change to the model, data, target group, or decision logic must be timestamped and attributed to a responsible person.
• Implement an **approval procedure** before market placement or deployment (e.g., four-eyes principle).
• **Audit note:** missing or outdated documentation constitutes a **compliance deficiency** and may result in withdrawal of **CE marking**.
• Integrate documentation into a **central audit repository** (e.g., according to **ISO/IEC 42001** or **ISO/IEC 23894**).

3 Human Oversight (Art. 14 EU AI Act)

• Involve **qualified human reviewers** before or after automated decisions, depending on risk level.
• Implement **technical control mechanisms**, such as:

- approval, verification, or stop functions (“Human-in-the-Loop” / “Human-on-the-Loop”);
- visualization of uncertainty levels (confidence scores).
  • Demonstrate effectiveness through:
- **training certificates** (Art. 4(4));
- **logs of human interventions**;
- **periodic effectiveness testing** within the monitoring process.

4 Technical and Organizational Measures (Arts. 12–15 EU AI Act)

• Implement **tamper-proof logging systems** with hash or WORM functionality.
• Conduct regular **security tests** (penetration testing, model drift analyses, adversarial testing).
• Define **redundancy and fallback strategies** for faulty or unreliable results.
• Establish a **lifecycle management framework** with defined revalidation intervals (e.g., every 6–12 months).
• Apply **role-based access control** and integrate with existing **information security** and **privacy management systems (ISMS / PIMS)**.
• Document results in the **Post-Market Monitoring Report** (Art. 24 EU AI Act).

Summary:
These four implementation dimensions – **risk management, documentation, human oversight, and technical measures** – together form the **operational backbone** of an effective AI compliance system. Organizations that integrate these components systematically ensure full legal compliance and strengthen **audit assurance**.

© A4Q Copyright 2025

5.4 Documentation and Evidence Obligations (Audit Readiness)

Comprehensive and traceable documentation is the core element of compliance for high-risk AI systems. It serves as proof to supervisory authorities, internal audit functions, and external certifiers that the system meets the requirements of the EU AI Act and is continuously monitored.

Guiding principle:
Anything not documented is considered not done.
Documentation, therefore, goes beyond archiving – it represents an active accountability process covering the AI system's entire lifecycle, from development and deployment to decommissioning.

1 Typical Evidence and Responsibilities

Type of Evidence	Purpose / Content	Responsible Role
Technical Documentation	Model, purpose, functionality, training and test data, validation, limitations	Provider / Development Lead
Risk Assessment	Identified risks, mitigation measures, approvals, and responsibilities	Compliance / AI Officer
Audit Trail & Logging	Traceability of inputs, decisions, interventions, and versions	IT Operations / System Owner
Change Log	Tracking of model, data, or parameter modifications	Technical Lead / QA
Training Records	Attendance logs, content, and competency assessments (Art. 4(4))	HR / AI Officer
Incident Reports	Notifications, root cause analyses, corrective measures (Arts. 23–24)	Compliance / Operations
Monitoring Reports	Performance data, drift detection, and corrective actions	Business Units / AI Governance Team

Together, these records form the **Conformity Dossier** (Arts. 17 ff.) and must remain **up-to-date, verifiable, and audit-ready at all times**.

2 Enhancing Audit Readiness

© A4Q Copyright 2025

An effective **audit management system** ensures that all documentation is **complete, standardized, and easily accessible**.
Key measures to enhance audit readiness include:
• **Standardized documentation schema** (e.g., ISO/IEC 42001 or ISO/IEC 23894).
• **Regular internal audits** – at least annually or after major system updates.
• **Audit trail visualization** (input → model processing → output → human approval).
• **Centralized repository** with controlled access and versioning.
• **Retention period:** minimum of **10 years** for high-risk systems (Art. 61).
• **Audit trail protection:** tamper-proof storage (e.g., hashing, blockchain, or WORM).
• **Audit communication plan:** predefined roles and procedures for authority or certification inquiries.

Practical tip:
Before an external audit, conduct an **internal pre-audit check** to identify and close documentation gaps in time.

3 Audit Readiness Checklist

This checklist can help you evaluate your organization's current level of audit readiness.

Audit Readiness Checklist

- Current system description, including purpose, version, responsible person, and scope of use.
- Risk register is complete, up to date, and linked to documented mitigation measures.
- Testing and validation protocols are archived and traceable.
- Logging is revision-proof and version-controlled.
- Incident response plan is documented and regularly tested.
- Monitoring reports are continuously maintained.
- Training for all operational roles has been conducted and documented.
- System changes and updates are traceably recorded.
- Approvals by responsible persons are logged.
- Audit schedule and responsibilities are defined in the annual plan.

Conclusion
Documentation is a **cornerstone of effective AI governance**.
By systematically recording **processes, data, decisions, and controls**, organizations can demonstrate compliance with the **EU AI Act** during audits and minimize the risk of non-conformities.

© A4Q Copyright 2025

A well-structured documentation system ensures **transparency, clear accountability, and traceability** – both internally and externally.

5.5 Example – Applying High-Risk AI Obligations in Practice

Scenario:

You take on the role of an **AI Compliance Officer** in a financial institution.
Your area of responsibility includes an **AI-powered credit scoring system** that automatically assesses customers' creditworthiness and provides recommendations for credit decisions.
According to **Annex III No. 5 of the EU AI Act**, this system falls within the scope of **high-risk AI systems**, as it directly affects the economic rights and obligations of individuals.

Objective of the Example:

The goal is to practice handling the **key compliance obligations** under **Articles 9–15 of the EU AI Act**, identify appropriate forms of evidence, and critically evaluate the **audit readiness** of the system.

1. Identification of Obligations

Obligation (Article)	Content / Objective	Reason for Selection
Art. 9 – Risk Management System	Systematic identification, evaluation, and control of all potential risks throughout the system's lifecycle	Credit decisions directly impact consumer rights; therefore, a formal risk management process is mandatory.
Art. 11 – Technical Documentation	Traceable description of the system's purpose, functionality, data, models, testing methods, and limitations	Without complete documentation, the system's functionality cannot be verified during an audit or complaint investigation.
Art. 14 – Human Oversight	Ensuring that humans can monitor, review, and intervene in the system when necessary	AI must not make automated decisions without human accountability; this safeguards fairness and prevents discrimination.

2. Required Evidence and Timing

Evidence	Purpose / Significance	When to Prepare / Update
AI Risk Register	Contains all identified risks, their evaluation (likelihood × severity), and defined mitigation measures.	After each major system change, at least every six months.

© A4Q Copyright 2025

Evidence	Purpose / Significance	When to Prepare / Update
Technical Dossier	Documents the model architecture, training data used, testing protocols, and system limitations.	Before market release, update upon model or data modification.
Approval and Review Logs	Proof that qualified personnel have reviewed and approved the system prior to deployment.	Before each deployment or major update.

3. Evaluation of Audit Readiness

The system is considered **audit-ready** if:
• all evidence is **complete, current, and version-controlled**,
• **roles and responsibilities** (owner, reviewer, approver) are clearly documented, and
• all relevant records can be presented to auditors **within 24 hours** upon request.

Justification:
These conditions reflect the principle of **accountability** under **Articles 11 and 61 of the EU AI Act**.
If any of these elements are missing – such as an outdated risk register or unsigned approval logs – the system is deemed **non-compliant** and requires immediate corrective action (e.g., post-documentation, revalidation).

Reflection and Possible Improvements

Reflection Question:
What organizational measures could help maintain long-term audit readiness?

Example Answers:
• Introduce an **annual internal audit** to review AI documentation.
• Use a **centralized audit repository** with access and version control.
• Require **refresher training** for AI Officers and operational departments.
• Implement a **compliance dashboard** that automatically flags upcoming document expirations.

Conclusion

High-risk AI systems, such as credit scoring, are **generally permitted**, but they are subject to **strict documentation and audit obligations**.
A **structured, documented, and verifiable process** throughout the entire lifecycle – from development to deployment and continuous monitoring – is essential.
Organizations that consistently comply with the requirements of **Articles 6–51 of the EU AI Act** ensure not only **legal conformity** but also strengthen **trust, accountability, and organizational reputation**.

© A4Q Copyright 2025

6 Risk Management and Quality Management Systems

⏱ **Duration:** 60 minutes

🎯 **Business Outcomes:**

- **BO 6.1:** Participants are prepared to contribute to the establishment or adaptation of an AI Risk Management System in alignment with **ISO/IEC 42001**.
- **BO 6.2:** Participants understand the importance of integrating AI processes into existing management systems (**QMS**, **ISMS**, **DSMS**) and how this integration supports compliance and quality assurance.

Learning Objectives (LOs)

- **LO 6.1 (K2):** Participants can explain the structure and purpose of an AI Risk Management System according to **Article 9 EU AI Act** and **ISO/IEC 42001**.
- **LO 6.2 (K2):** Participants can describe the interconnections between the obligations of the EU AI Act and existing management systems (QMS, ISMS, DSMS).
- **LO 6.3 (K1):** Participants can identify the phases of a continuous AI risk management cycle (risk assessment, mitigation, monitoring, improvement).
- **LO 6.4 (K1):** Participants can explain how documentation, monitoring, and audits contribute to audit readiness.
- **LO 6.5 (K1):** Participants know the fundamental steps of an AI risk management cycle.

Key Terms:
ISO/IEC 42001 (AI Management System), ISO/IEC 23894 (AI Risk Management), risk management cycle, proportionality, lifecycle coverage, lessons learned, control report, stakeholder analysis, accountability, traceability, quality management (QM), ISMS, DSMS

Introduction
The EU AI Act requires organizations, under Articles 9 and 17–23, to establish a systematic Risk Management System for high-risk AI systems. This system must cover the entire lifecycle – from design and development to operation and decommissioning.

© A4Q Copyright 2025

International standards such as ISO/IEC 23894 (Risk Management for AI) and ISO/IEC 42001 (AI Management System – AIMS) provide recognized frameworks and methodologies for implementing these legal obligations.
They translate the regulatory requirements of the AI Act into auditable and verifiable management processes.

The objective of this chapter is to provide participants with a practical understanding of the core principles of AI risk management and to illustrate how these can be integrated into existing Quality (QMS), Information Security (ISMS), and Data Protection Management Systems (DSMS) to ensure compliance, accountability, and continuous improvement.

6.1 Core Principles of AI Risk Management

A Risk Management System under **Article 9 of the EU AI Act** must meet the following key requirements:

- **Lifecycle coverage:** Analysis across all stages – design, training, deployment, monitoring, and decommissioning.
- **Regular updates:** Periodic review after any changes to the model, data, or intended purpose.
- **Documentation and traceability:** All evaluations and mitigation actions must be recorded in writing.
- **Proportionality:** The depth and scope of the process must correspond to the level of risk involved.

Main objectives of the system:

Objective	Description
Protection of fundamental rights	Prevention of discrimination, deception, and manipulation.
Technical safety	Ensuring robust, reliable, and fault-tolerant system operation.
Traceability	Every decision must be explainable and verifiable after deployment.
Accountability	Clear definition of roles, responsibilities, and escalation paths within the organization.

© A4Q Copyright 2025

Thus, AI risk management serves not only to fulfill legal obligations but also to ensure **quality assurance, organizational accountability**, and to **build trust** with customers, regulators, and the general public.

6.2 The Risk Management Cycle According to ISO/IEC 23894 and the EU AI Act

The AI-Act-compliant risk management process follows a **continuous cycle** of identifying, assessing, controlling, and monitoring risks.

Phase	Key Activities	Reference to Art. 9 EU AI Act
1 – Define context and objectives	Determine system purpose, stakeholders, legal framework, and relevance to fundamental rights.	Art. 9(2)(a)
2 – Identify risks	Detect technical, organizational, and ethical risks (e.g., bias, malfunction, data protection).	Art. 9(2)(b–c)
3 – Analyze and evaluate risks	Assess probability and impact; prioritize according to risk category.	Art. 9(2)(d)
4 – Risk control and mitigation	Implement technical and organizational controls (e.g., fallback mechanisms, human oversight, logging).	Art. 9(3)
5 – Monitoring and improvement	Continuous monitoring per Art. 24; integrate lessons learned and control reports.	Art. 9(4)

This process must be repeated **at least annually** or after **substantial modifications**, such as the introduction of new training data, model updates, or changes in purpose.

6.3 Integration into Existing Management Systems

An isolated AI risk management system often results in **redundancy and inefficiency**. Therefore, close integration with existing management systems is recommended, particularly with **ISO/IEC 42001 (AIMS)**, **ISO 9001 (QMS)**, **ISO/IEC 27001 (ISMS)**, and **ISO/IEC 27701 (DSMS)**.

Management System	Purpose	Contribution to AI Compliance
QMS (ISO 9001)	Quality management and process control	Ensures consistent documentation and regular audits.

© A4Q Copyright 2025

Management System	Purpose	Contribution to AI Compliance
ISMS (ISO/IEC 27001)	Information security, confidentiality, and integrity	Protects training and operational data from manipulation and loss.
DSMS (ISO/IEC 27701 / GDPR)	Data protection compliance	Aligns Data Protection Impact Assessments (DPIA) with AI risk assessment.
AIMS (ISO/IEC 42001)	AI governance and risk management	Central documentation and evidence framework for compliance with the Arts. 9 and 17–23 of the EU AI Act.

Integration creates a **"system of systems"** in which processes, audit cycles, and roles are coordinated. This results in a **coherent governance framework** that combines **technical and legal controls**, enhances efficiency, and strengthens overall compliance resilience.

6.4 Documentation and Evidence Obligations

Articles 17–23 of the EU AI Act require comprehensive documentation and evidence management to demonstrate **conformity** and ensure **audit readiness**.

Mandatory documents include:

1. Risk management plan with assessment matrix and risk criteria.
2. Technical documentation in accordance with **Article 11** (architecture, data, testing, limitations).
3. Logs of monitoring activities, incident reports, and corrective actions.
4. Up-to-date **Declaration of Conformity** under **Article 19**, including version history and responsible persons.
5. Links to internal **audit reports** from related management systems (QMS/ISMS).

All documentation must be:
• **traceable, complete, and version-controlled**,
• **centrally archived** with restricted access, and
• **made available within 48 hours** in the event of an audit or regulatory inquiry.

Documentation is a continuous process and must be updated whenever there are changes to models, data, use contexts, or governance structures.
According to ISO/IEC 42001 (Sections 7.4 and 9.2), documentation is an integral part of the Artificial

© A4Q Copyright 2025

Intelligence Management System (AIMS) – serving as the information backbone for audits, reviews, and management assessments.

To ensure auditability, all records should be structured, machine-readable (e.g., PDF/A, XML), and clearly linked to a specific system version and a responsible individual.
Responsibility for maintaining and ensuring completeness lies with the AI Compliance Officer or the documentation manager within the Quality Management System (QMS).

6.5 Governance, Roles, and Responsibilities

An effective AI Risk Management System requires clear governance structures and well-defined responsibilities.
Only when roles, decision-making authority, and communication channels are established and documented can the system operate effectively in accordance with Articles 9 and 17–23 of the EU AI Act.

Role	Core Tasks and Responsibilities
AI Compliance Manager / AI Officer	Overall coordination of the risk management process, maintenance of the risk register, monitoring effectiveness of mitigation measures, preparing internal and external audits, and liaising with authorities and certification bodies.
Subject Matter Experts / System Owners	Identify and assess new operational risks, report incidents and model changes, and ensure technical modifications are documented and approved.
Data Protection and Security Officers	Align Data Protection Impact Assessments (DPIAs) with AI risk assessments, participate in incident response processes, and ensure consistency with ISMS and DSMS requirements.
Quality Management (QMS) Officers	Integrate AI risk management into existing audit and documentation workflows, harmonize procedures, and review cycles.
Ethics or Compliance Committee (optional)	Evaluate ethical implications, resolve conflicts of objectives (e.g., accuracy vs. fairness), and approve sensitive systems or high-risk use cases.
Management / Executive Board	Approve the risk strategy, establish governance policies, allocate resources, and receive regular reports on the maturity level of the AI compliance system.

© A4Q Copyright 2025

All roles must be complemented by documented deputy and escalation procedures.
It is recommended to represent responsibilities using a RACI Matrix (Responsible – Accountable – Consulted – Informed), which should be reviewed regularly and updated after organizational changes.

This governance approach ensures that decisions are transparent, auditable, and traceable, forming the foundation for effective internal control and continuous improvement within the Artificial Intelligence Management System (AIMS) in line with ISO/IEC 42001.

6.6 Importance of Integration for Compliance and Quality

Integrating AI risk management into existing management systems (e.g., QMS, ISMS, DSMS) is a key success factor for sustainable compliance.
It ensures that obligations under the EU AI Act are met within established organizational structures rather than through isolated processes.

Benefits of integration:

- **Reduced duplication of effort:** Data Protection Impact Assessments (DPIAs) and AI risk assessments can be performed jointly, avoiding redundant processes.
- **Consistency of evidence:** Documentation, reports, and audit logs follow unified versioning, approval, and archiving standards.
- **Improved traceability:** Harmonized processes and synchronized audit cycles ensure full traceability of decisions and changes.
- **Enhanced quality and efficiency:** Risks are identified earlier, mitigation measures are documented systematically, and preventive corrections are triggered throughout the lifecycle.
- **Holistic governance:** Integration strengthens the connection between technical, legal, and organizational controls – a core requirement under **ISO/IEC 42001**.

Organizations that implement this integration effectively can achieve a “Presumption of Conformity” under Article 40 of the EU AI Act.
This enables them to fulfill regulatory and certification requirements efficiently while demonstrating higher process reliability, product quality, and regulatory maturity.

© A4Q Copyright 2025

7 Conformity Assessment and CE Marking

⏱ **Training Duration:** 80 minutes

🎯 **Business Outcomes**

- **BO 7.1:** Participants develop an understanding of conformity assessment routes and are prepared to support their practical application.
- **BO 7.2:** Participants are able to support the CE marking process and the registration of AI systems in the EU database.

Learning Objectives (LOs)

- **LO 7.1 (K2):** Participants can describe internal and external conformity assessment procedures according to Articles 43–51 of the EU AI Act.
- **LO 7.2 (K2):** Participants can assess when a notified body must be involved.
- **LO 7.3 (K2):** Participants can explain the content of technical documentation and its relevance for audits.
- **LO 7.4 (K1):** Participants can outline the CE marking process for high-risk AI systems.
- **LO 7.5 (K1):** Participants can identify the registration process in the EU database and the corresponding responsibilities within the organization.
- **LO 7.6 (K3):** Participants can evaluate obligations following significant system changes and initiate a re-assessment.
- **LO 7.7 (K1):** Participants are familiar with the key elements of a conformity assessment under Article 43 of the EU AI Act.

Key Terms

Conformity assessment, technical documentation, EU declaration of conformity, CE marking, notified body, provider obligations, market surveillance, Article 43 EU AI Act, verification procedures, internal control procedure, audit trail, and evidence of compliance.

Introduction

Conformity assessment is the central mechanism for the legal authorization of high-risk AI systems under the EU AI Act.

© A4Q Copyright 2025

It verifies whether a system meets all legally required obligations—from data quality and risk management to transparency and human oversight.

The conformity process concludes with the CE marking and registration of the system in the European database for AI systems.
It represents the critical step between development and market placement, ensuring that only compliant, safe, and trustworthy AI systems enter the EU market.

7.1 Fundamentals of Conformity Assessment (Art. 43 EU AI Act)

The purpose of the conformity assessment is to objectively verify that an AI system meets all essential requirements of the Regulation, particularly with regard to safety, data quality, transparency, human oversight, and risk management.
The conformity process, therefore, serves as a bridge between technical development and legal market authorization.

Types of Conformity Assessment Procedures

Type of Procedure	**Key Characteristics**	**Typical Application Cases**
Internal Conformity Assessment	Conducted under the provider's own responsibility. Includes preparation of the technical documentation, execution of internal testing, and issuance of the EU Declaration of Conformity.	Standard cases without critical social or safety implications, e.g., AI-assisted HR processes or credit-scoring systems with a limited operational scope.
Assessment by a Notified Body	External evaluation performed by an accredited organization ("Notified Body"). The body reviews the provider's quality management system, performs sample-based technical inspections, and certifies compliance.	Highly critical applications such as biometric identification, medical diagnostics, or safety-related infrastructure control.

In both cases, **the provider remains fully responsible** for the **accuracy, completeness, and currency** of all documentation—even when an external body is involved.

© A4Q Copyright 2025

Steps of the Conformity Assessment Process

1. Preparation and Documentation
Collect all evidence related to risk management, data quality, human oversight, and robustness.
Prepare the **technical dossier** according to Annex IV of the EU AI Act.

2. Execution of the Assessment

- *Internal:* Conducted by internal responsible experts (e.g., AI Compliance Manager, Quality Management).
- *External:* Audited and reviewed by a Notified Body.

3. Results and Certification
Prepare a **conformity report** and, where applicable, obtain an **EU-type examination certificate**.
Based on this evidence, the **EU Declaration of Conformity** is issued and the **CE mark** affixed.

4. Follow-up and Monitoring
Ensure continuous supervision, especially when system modifications or new training data are introduced (**Post-Market Monitoring**).

Decision Logic for Selecting the Procedure

The choice between an internal and external conformity assessment depends on three main factors:

1. **Risk Classification of the System (Articles 6 ff. EU AI Act)**
    - Only **high-risk AI systems** are subject to formal conformity assessment.
    - Systems classified as **limited or minimal risk** are exempt from CE marking.
2. **Type of Application (Annex III EU AI Act)**
   Within the high-risk category, the AI Act differentiates between:
    - **Standardized high-risk applications** (e.g., HR or credit scoring systems) → internal assessment permitted.
    - **Safety- or rights-critical applications** (e.g., biometric identification, medical devices, or critical infrastructures) → external assessment by a Notified Body required.
3. **Existence of a Certified Management System**
   If the provider operates a recognized **Quality or AI Management System** (e.g., ISO/IEC 42001 or ISO 9001), the internal assessment may be considered equivalent.
   If such a system is not in place, **involvement of a Notified Body** is generally mandatory.

© A4Q Copyright 2025

Summary Table

Conditions	Applicable Procedure	Example
High-risk system, standardized use, certified internal QMS in place	Internal conformity assessment	AI for candidate analysis or credit scoring
High-risk system with safety- or fundamental-rights relevance, no certified management system	Assessment by a Notified Body	Facial recognition in public spaces, medical diagnostic software
Limited or minimal-risk system	No formal CE assessment required	Chatbot with user disclosure notice

Practical Example

A provider of an AI-based recruitment tool performs an internal conformity assessment.
Since the system falls under Annex III, Section 4 (“Management of employment relationships”), the provider documents all risk-control measures and prepares the required technical documentation.

However, if a later version of the system included biometric candidate verification, an assessment by a Notified Body would be mandatory.

Recommendation

Conformity assessment is not a one-time event, but a continuous process throughout the system’s entire lifecycle.
It constitutes the core of compliance evidence during audits and is a prerequisite for CE marking and registration in the EU database for AI systems.

7.2 Contents of the Technical Documentation (Articles 11 & Annex IV)

The technical documentation is the central compliance record within the conformity assessment process.
Its purpose is to demonstrate to authorities and notified bodies that the AI system meets all essential requirements of the EU AI Act.
It must be complete before market placement, continuously updated, and readily available for inspection at any time.

© A4Q Copyright 2025

A. Mandatory Components (Legally Required under Article 11 in conjunction with Annex IV of the EU AI Act)

These elements are **compulsory** for successfully completing the conformity assessment:

1. **Description of the AI System**
   – Intended purpose, system architecture, core functionalities, and limitations of use.
   (Rationale: required for risk classification and functional traceability.)

2. **Risk Management Procedures and Results (Article 9)**
   – Documentation of identified risks, their severity ratings, and the effectiveness of mitigation measures.
   (Mandatory for all high-risk AI systems.)

3. **Data and Data Quality Evidence (Article 10)**
   – Description of training, validation, and testing data; sources; representativeness; and bias-control methods.
   (Essential for fairness, robustness, and non-discrimination.)

4. **Evidence of Technical Safety, Accuracy, and Robustness (Article 15)**
   – Test results, performance metrics, safety evaluations, and cybersecurity controls.

5. **Description of Human Oversight Mechanisms (Article 14)**
   – Explanation of how human control, intervention, and supervision are technically implemented.

6. **User Manual and Terms of Use**
   – Clear instructions for proper operation, including limitations and warnings.
   (Required to prevent misuse and liability risks.)

7. **Post-Market Monitoring Concept (Article 61)**
   – Description of how the system will be monitored after market placement, including feedback and incident reporting processes.

8. **Draft EU Declaration of Conformity (Article 48)**
   – Formal statement by the provider confirming compliance with applicable EU AI Act provisions.
   (Prerequisite for CE marking.)

B. Optional or Supporting Evidence (Recommended but Not Mandatory)

These elements are **not explicitly required** by law but are **strongly recommended** to enhance auditability, transparency, and traceability:

9. **Assessment of Alignment with Harmonized Standards**
   – Reference to ISO/IEC 42001 (AI Management System), ISO/IEC 23894 (AI Risk Management),

© A4Q Copyright 2025

or DIN SPEC 92001-2.
(Optional, but supports the "Presumption of Conformity," facilitating audits and CE evaluation.)

10. **Detailed Logging and Monitoring Concepts**
– Specification of log structure, access controls, and audit trail mechanisms.
(Recommended for continuous audit readiness and security verification.)

11. **Evidence of Internal Quality Management**
– Proof that an operational Quality Management System (e.g., ISO 9001 or ISO/IEC 42001) is in place.
(Facilitates internal conformity assessments under Article 43(2)(b).)

Rationale for Differentiation

• Mandatory components are defined directly in **Articles 9–15** and **Annex IV** of the EU AI Act.
• Optional components, while not legally required, are often requested by **notified bodies** to enable a full evaluation or to reduce time and cost during internal audits.

Recommendation:
Organizations should align with harmonized standards, as they represent recognized proof of the *Presumption of Conformity* and significantly reduce regulatory and audit risks.

Recommendation: Alignment with Harmonized Standards

When preparing technical documentation and establishing an AI Management System, organizations should follow the harmonized standards recognized by the European Commission.
These standards are published in the *Official Journal of the EU* and provide the legal foundation for the Presumption of Conformity—the assumption that an AI system complies with the EU AI Act if it is developed and operated according to these standards.

Recommended Harmonized Standards for the EU AI Act

Standard	Title / Focus	Relation to the AI Act	Publication / Status
ISO/IEC 42001:2023	*Artificial Intelligence Management System (AIMS)* – Requirements for establishing, implementing, maintaining, and continually	Corresponds to Articles 17–23 (Quality and Risk Management). Serves as a basis for internal conformity assessment.	Published 2023, ISO certifiable since Q2 2024.

© A4Q Copyright 2025

Standard	Title / Focus	Relation to the AI Act	Publication / Status
	improving an AI management system.		
ISO/IEC 23894:2023	*Artificial Intelligence – Guidance on Risk Management* – Integrates AI-specific risks into existing management systems.	Covers Article 9 (AI Risk Management System).	Published 2023, recommended for international application.
ISO/IEC 22989:2022	*Artificial Intelligence – Concepts and Terminology* – Establishes shared definitions for documentation and audits.	Supports Article 11 (Technical Documentation) and Annex IV.	Published 2022, foundational for subsequent standards.
ISO/IEC 23053:2022	*Framework for Machine Learning (ML) – Lifecycle Management* – Lifecycle model for ML systems.	Supports Article 10 (Data) and Article 15 (Robustness).	Published 2022, under revision for AI Act alignment (expected 2026).
ISO/IEC 24028:2020	*Overview of Trustworthiness in Artificial Intelligence* – Guidance on safety, resilience, and reliability.	Complements Article 15 (Cybersecurity and Robustness).	Published 2020, revision planned for 2026.
DIN SPEC 92001-1:2020	*Quality Requirements for AI Systems – Fundamentals*	National pre-standard to ISO/IEC 42001; practical for German organizations.	Published 2020, considered an interim reference.
DIN SPEC 92001-2:2021	*Quality Requirements for AI Systems – Testing Criteria*	Supports audit preparation and compliance verification.	Published 2021.
ISO/IEC 27001:2022	*Information Security Management System (ISMS)*	Supports data security obligations under Article 15.	Published 2022 (current edition).
ISO/IEC 27701:2019	*Privacy Information Management System (PIMS)* – Extension to ISO 27001.	Complements data protection obligations under Articles 10 and 15.	Published 2019, revision expected 2026.

© A4Q Copyright 2025

Note on Harmonization (Status 2025)

- The **European Commission** and **CEN/CENELEC JTC 21** are currently converting these ISO standards into **European harmonized standards (EN-ISO)**.
- The first set of harmonized standards for the AI Act is expected to be published in the **first half of 2026** in the Official Journal of the EU.
- Until then, the ISO/IEC standards listed above are accepted as **recognized best practice** and are already used by **notified bodies** during audits.

Why These Standards Matter

- They structure and standardize the technical documentation, simplifying audits.
- They reduce interpretation gaps during inspections and regulatory reviews.
- They enable integration of AI and quality management, supporting internal conformity assessments under Article 43(2)(b) of the EU AI Act.
- They serve as credible **evidence of conformity** in case of disputes or regulatory audits.

7.3 CE Marking Procedure (Article 49 EU AI Act)

After successfully completing the conformity assessment, the provider must issue a written EU Declaration of Conformity confirming that the AI system meets all applicable requirements of the Regulation.
Only then may the CE marking be affixed—it serves as the visible proof of regulatory compliance and market authorization within the EU.

Steps for CE Marking

Step	Content / Rationale
1. Completion of the Conformity Assessment (internal or external)	Evidence that the system meets the requirements of Articles 9–15. Based on the complete technical dossier as per Annex IV.
2. Preparation and Signature of the EU Declaration of Conformity (Article 48)	Legally binding declaration by the provider confirming compliance. Must include the provider's name, system identification, applied standards, and date of issue.

© A4Q Copyright 2025

Step	Content / Rationale
3. Affixing the CE Marking	The CE symbol may only be affixed after the declaration—on the user interface, packaging, or documentation, depending on the system type.
4. Registration in the EU Database for High-Risk AI Systems (Article 71)	Mandatory step before placing the system on the market. The entry includes provider details, intended purpose, risk category, notified body (if applicable), and date of declaration.
5. Retention of Documentation for at Least 10 Years (Article 50)	Long-term recordkeeping for market surveillance, audits, and liability purposes. Applies even after system decommissioning or transfer of ownership.

Important Notes

- The CE marking applies only to the assessed system version in its evaluated configuration.
- Substantial modifications—such as new training data, altered models, deployment in new domains, or integration into other products—require a new conformity assessment.
- The provider must determine whether a change qualifies as “substantial” under Article 43(4).

7.4 Role of Notified Bodies

Notified Bodies are organizations accredited by EU Member States and subsequently listed by the European Commission in the NANDO database (New Approach Notified and Designated Organisations). They are responsible for conducting external conformity assessments for high-risk AI systems when internal assessment is insufficient or legally excluded.

Responsibilities and Evaluation Areas

- Evaluation of the provider’s risk management and quality management systems
- Sampling review of technical documentation and test reports
- Verification of testing and validation results for accuracy and consistency
- On-site audits at the provider’s or operator’s facilities
- Issuance of an EU type-examination certificate, which serves as the basis for CE marking

© A4Q Copyright 2025

Examples of Notified Bodies (EU-wide)

- TÜV Rheinland, DEKRA (Germany)
- Bureau Veritas, SGS (France/Switzerland – EU recognized)
- Applus+ Laboratories (Spain)
- IMQ S.p.A. (Italy)
- VTT Expert Services Ltd (Finland)

All bodies listed in the European Commission's NANDO register may operate throughout the EU.
The choice of body depends on its scope of accreditation and the sector involved (e.g., biometrics, medical applications, critical infrastructure).

7.5 Registration in the EU Database for High-Risk AI Systems (Article 71)

Before a high-risk AI system can be placed on the market or put into service, it must be registered in the EU's central database for AI systems.
This registration is mandatory and serves as official proof that the system has successfully passed a conformity assessment.

Information to Be Submitted

- Provider's name and contact details (manufacturer or distributor)
- System name and description, including its intended purpose and application domain
- System's risk category and reference to the relevant Annex III section
- Type of conformity procedure (internal or external under Article 43)
- Identification of the Notified Body, if applicable
- Date and reference number of the EU Declaration of Conformity and CE marking

Purpose of the Database

- The EU database promotes transparency, market oversight, and traceability. It enables:
- Authorities to efficiently monitor compliance and perform market surveillance,
- Companies and clients to verify authorized AI systems, and
- The public to access information on which high-risk AI systems are deployed in the EU.

© A4Q Copyright 2025

Registration is performed electronically via the EU portal operated by the European Commission.
Only after successful registration may the system be placed on the market or marketed with the CE marking.

7.6 Handling of Substantial Modifications (Article 43(4))

An AI system is considered compliant only in the configuration that was originally assessed and CE-marked.
If the system undergoes substantial modification after the conformity assessment, a new conformity assessment must be carried out before further use or marketing.

Examples of Substantial Modifications

- **Change of intended purpose or functional logic**, e.g., using an AI system originally designed for candidate screening to perform employee performance evaluations.
- **Use of new training or validation data** whose quality, representativeness, or bias characteristics have not been verified.
- **Alteration of the system architecture** or integration into new software/hardware platforms that affect behavior, safety, or performance.
- **Deployment in a different application domain or legal context**, e.g., transferring an HR screening system to medical fitness assessments.

Responsibility

The provider (manufacturer or distributor) is responsible for determining whether a modification is substantial.

They must document:

- The nature of the change,
- Whether it affects the system's risk, data, or functional profile, and
- Which additional evidence may be required for re-assessment.

Practical Recommendation

Organizations should establish a change management procedure that automatically evaluates technical updates, retraining processes, or new features for their potential compliance relevance.
This approach helps prevent unintentional non-compliance and mitigate audit risks at an early stage.

© A4Q Copyright 2025

7.7 Link to Quality and Management Systems

The EU AI Act introduces the principle of “Presumption of Conformity”, meaning that if a company applies harmonized European or international standards during the development, operation, and monitoring of its AI system, it is presumed to comply with the relevant legal requirements of the AI Act.
This greatly facilitates the conformity assessment process and accelerates CE marking.

Relevant Standards and Management Systems:

- **ISO/IEC 42001:2023 – Artificial Intelligence Management System (AIMS)**
  Provides a structured framework for establishing, operating, and maintaining an AI management system.
- **ISO/IEC 23894:2023 – AI Risk Management**
  Defines a systematic approach to AI risk management aligned with **Article 9 of the EU AI Act**.
- **ISO/IEC 27001:2022 / ISO/IEC 27701:2019 – Information and Privacy Management Systems**
  Ensures data security and confidentiality in accordance with **Articles 10 and 15**.
- **DIN SPEC 92001-1/-2:2020/2021 – Quality Requirements for AI Systems**
  German guideline for documentation, testing, and audit preparation.

Advantages for Organizations:

Applying these standards creates structure and traceability:

- simplifies audits and market surveillance,
- reduces interpretation inconsistencies among notified bodies,
- and can accelerate CE marking.

7.8 Practical Example: Conformity Route of an HR Screening Tool

This example illustrates a typical conformity assessment process for a high-risk AI system in the HR domain – specifically, an AI-based tool used to automatically pre-screen job applications.
The system falls under Annex III No. 4 (Employment, Worker Management, and Access to Employment) of the EU AI Act and therefore requires a formal conformity assessment and CE marking.

© A4Q Copyright 2025

Step	Objective / Content	Responsibility in the Organization	Required Document / Evidence
1. Risk Assessment (Arts. 6–9)	Identify whether the system qualifies as high-risk and describe potential impacts on fundamental rights and fairness.	AI Compliance Manager in coordination with Data Protection and HR	Risk Report (including justification for classification and Annex III reference)
2. Implementation of Risk Management (Art. 9)	Establish a continuous risk monitoring process, define mitigation measures, and testing mechanisms.	Development Team with Quality Management	Risk Register with action matrix and assigned responsibilities
3. Preparation of Technical Documentation (Art. 11, Annex IV)	Comprehensive documentation of the system, data sources, training processes, testing protocols, and human oversight mechanisms.	HR Department + Quality Assurance	Technical Dossier according to Annex IV
4. Internal Conformity Assessment (Art. 43(2))	Verify completeness and accuracy of evidence within the dossier, conduct internal audit, and prepare the conformity report.	AI Officer / Compliance Team	Internal Conformity Report with review results
5. EU Declaration of Conformity (Art. 48)	Formal declaration confirming compliance with all requirements (Arts. 9–15).	Management / Legal Representative	Signed EU Declaration of Conformity (legally binding)
6. Registration in the EU Database (Art. 71)	Official registration in the EU database for high-risk AI systems – a prerequisite for placing the system on the market.	AI Officer / Compliance	Registration form with system ID, CE number, and risk category
7. CE Marking (Art. 49)	Visible proof of conformity on the product, interface, or accompanying documentation.	Product Management	CE Label and supporting documentation

© A4Q Copyright 2025

Step	Objective / Content	Responsibility in the Organization	Required Document / Evidence
8. Annual Audit / Review (Art. 61, Post-Market Monitoring)	Verify continued compliance (e.g., after updates, new data, or process changes).	Quality & Compliance / Internal Audit Function	Audit Report + Updated Risk Register

Key Learning Points:

- Responsibility remains with the **provider**, even if individual tasks are distributed internally.
- The **documentation chain** (risk → mitigation → assessment → declaration → audit) must be complete and verifiable.
- Regular reviews are necessary, as AI systems evolve through retraining and software updates.
- Following these steps ensures a **legally sound CE marking** and protects the company from **liability and reputational risks**.

7.9 Practical Recommendations

To ensure that conformity assessment is efficient, transparent, and audit-proof, companies should implement the following best practices.
These recommendations support the ongoing maintenance of CE conformity and reduce both liability and audit risks.

1. **Early Involvement of Legal and Compliance Functions**
   Engage legal and compliance experts early in the planning phase of any AI project.
   This ensures that **risk classification, data requirements, and documentation obligations** are correctly defined from the outset.
2. **Maintain a Conformity Assessment Checklist (Arts. 9–23 EU AI Act)**
   A standardized checklist helps systematically track all required evidence (risk management, data quality, human oversight, etc.) and identify gaps in time.
3. **Integration with Existing Management Systems**
   Embedding AI compliance processes into existing frameworks such as **Quality Management (ISO 9001)**, **Information Security (ISO/IEC 27001)**, or **AI Management Systems (ISO/IEC 42001)** creates synergies, reduces duplication, and facilitates audits.

© A4Q Copyright 2025

4. **Regular Internal CE Compliance Audits**
   Conduct internal audits periodically to identify changes, weaknesses, or deviations early.
   Documented audit reports serve as valuable evidence for **authorities and certification bodies**.

5. **Establish a Central Document Repository with Version Control and Audit Trail**
   All conformity-related records (risk, testing, validation, and approval evidence) should be maintained in a controlled repository.
   Versioning and change logs ensure **traceability and evidential strength** during audits.

© A4Q Copyright 2025

8 Transparency Obligations for Limited-Risk Systems (Art. 52 EU AI Act)

⏱ **Instruction Time:** 90 minutes

🎯 **Business Outcomes (BOs)**

- **BO 8.1:** Participants are prepared to apply transparency requirements for chatbots, emotion recognition, and deepfakes.
- **BO 8.2:** Participants acquire the ability to evaluate and adapt labeling systems within interface design to ensure compliance.

Learning Objectives (LOs)

- **LO 8.1 (K2):** Participants can explain the transparency requirements under Article 52 of the EU AI Act and describe their significance for limited-risk systems.
- **LO 8.2 (K2):** Participants can differentiate between transparency requirements for high-risk systems (Arts. 13–14) and limited-risk systems (Art. 52).
- **LO 8.3 (K3):** Participants can design suitable interface labels and user notifications to implement transparency obligations in practice.
- **LO 8.4 (K3):** Participants can assess existing systems (e.g., chatbots, emotion recognition, generative media) for compliance with labeling obligations.
- **LO 8.5 (K1):** Participants know the fundamental transparency obligations for limited-risk systems and understand their purpose in strengthening user trust.

Key Terms:
Limited risk, transparency obligation, labeling requirement, human interaction, chatbot disclosure, emotion recognition, deepfake labeling, information duty, consumer protection, accountability, documentation evidence.

Introduction

Limited-risk systems such as **chatbots, emotion recognition tools, and deepfake generators** are generally permitted under the EU AI Act but are subject to specific **information and labeling obligations** (Art. 52).

© A4Q Copyright 2025

The purpose of these provisions is to protect users from deception and ensure that they can always recognize when they are interacting with an AI system or consuming AI-generated content.

Transparency is therefore not an ethical option but a legal requirement that must be visibly implemented in both the user interface and system communication.

Note: Classification of Emotion Recognition and Biometric Categorization
Emotion recognition and biometric categorization systems are not automatically classified as limited-risk AI. Their risk level depends on the use context and the impact on affected individuals:

- **Limited-Risk (Art. 52(2) EU AI Act):**
  If detection is used solely for informational or convenience purposes (e.g., mood detection in vehicles, customer service bots analyzing friendliness), the transparency obligation applies, but no CE marking or conformity assessment is required.
- **High-Risk (Art. 6 in conjunction with Annex III):**
  If emotion recognition or biometric categorization influences decisions regarding education, employment, access to services, or safety, it is classified as a high-risk AI system.
  In such cases, the extended obligations of Articles 9–24 (risk management, documentation, human oversight, CE marking) apply.
- **Prohibited (Art. 5(1)(a–b)):**
  Use is forbidden if emotional states are exploited to manipulate individuals covertly or to target vulnerable groups (e.g., children) for behavioral influence.

8.1 Article 52 EU AI Act – Transparency Obligations

Article 52 establishes three key transparency obligations:

Obligation Area	Description	Examples
a) Interaction Recognition	Individuals must be able to recognize when they are interacting with an AI system.	Chatbots, voicebots, virtual assistants
b) Emotion Recognition & Biometric Categorization	Users must be informed when their emotions or personal characteristics are being analyzed.	Camera-based customer analysis, voice, or gaze tracking

© A4Q Copyright 2025

Obligation Area	Description	Examples
c) Deepfakes & AI-Generated Media	AI-generated or manipulated content must be clearly identified as such.	AI videos, synthetic voices, generated images

Objective: Prevent deception, foster user trust, and protect fundamental rights.

8.2 Application Areas and Labeling Obligations

The practical requirements for transparency and labeling vary depending on the type of AI system.
Article 52 requires providers and deployers to ensure clear and understandable disclosures and labels in the following three main application areas.

a) Chatbots and Voicebots

Chatbots and voice-based assistants are classified as **limited-risk systems**, provided they do not make decisions with legal or economic consequences.
They are subject to the **information obligation** under **Article 52(1)** of the EU AI Act.
The goal is to ensure that users can always recognize that they are communicating with an AI system.

Recommended Implementation Measures:

- Clearly disclose the use of AI at the start of the interaction, e.g.:
  "You are interacting with an AI-based assistant."
- Repeat the reminder during long sessions or when topics change.
- Offer an **opt-out** option or transfer to a **human agent**.
- Log user information and consent within the system or session log.

b) Emotion Recognition Systems

Systems that analyze facial expressions, voice, or physiological signals to infer emotional states fall under **Article 52(2)** of the EU AI Act.
They may only be used if users have been clearly informed **beforehand** and there is a **lawful basis** (e.g., consent or legitimate interest).

© A4Q Copyright 2025

A lawful basis means that the processing of personal data—especially biometric or sensitive information—complies with the **General Data Protection Regulation (GDPR)**. This may include:

Consent (Art. 6(1)(a) GDPR):
The individual explicitly and voluntarily consents to emotion analysis after being informed about the purpose and scope of data processing.

Legitimate Interest (Art. 6(1)(f) GDPR):
Use serves a legitimate, clearly defined purpose (e.g., improving service quality) without disproportionately affecting individual rights.
In this case, a **balancing test** and possibly a **Data Protection Impact Assessment (DPIA)** are required.

If these legal conditions are **not met**, the system **may not be used or activated**.

Required Transparency Measures:

- Pre-information about purpose, type, and scope of data analysis, e.g.:
- *"This system analyzes facial and vocal expressions to detect emotional states."*
  Prohibition of **covert analysis** without explicit consent.
- Storage of emotion data only if **technically necessary** and **legally permitted**.
- Transparent display of evaluation metrics, such as probabilities:
  "Probability of positive emotion: 73%."

Note:
If emotion recognition is used in sensitive contexts (e.g., employment, education, law enforcement), it may be classified as a high-risk AI system under Art. 6 in conjunction with Annex III, triggering full obligations under Arts. 9–24 (risk management, documentation, human oversight, CE marking).

c) Deepfakes and Generative Media

For AI-generated or AI-modified content (e.g., images, videos, or audio), Article 52(3) applies.
The goal is to prevent deception and make the origin of content transparent.

Required Labeling Measures:

- Visible overlays or text markers such as *"AI-generated," "synthetic content,"* or *"created using artificial intelligence."*
- Machine-readable metadata labeling (e.g., IPTC/XMP tag ai-generated=true).

© A4Q Copyright 2025

- Responsibility for proper labeling lies with **both creators and distributors** (e.g., marketing or media agencies).

Exceptions apply only to authorized uses in public safety or law enforcement, as outlined in Art. 52(3), second subparagraph.

8.3 Design Recommendations for Interfaces and Labeling

To comply with the transparency obligations under Article 52, indicators of AI-generated content or interaction must be designed so that all users can clearly perceive, understand, and technically verify them. The table below outlines key design principles for legally compliant and user-friendly interface labeling.

Principle	Description	Example in UI Design
Visibility	Labels must be immediately noticeable without user action.	"AI Response" label above chat history; "AI-generated" watermark on images or videos.
Clarity	Wording should be plain, neutral, and easily understood to prevent confusion.	Text note: "This message was automatically generated by an AI system."
Consistency	Labels must be uniform across all channels to ensure recognition and trust.	Same style and wording on websites, apps, and email bots.
Persistence	Indicators must remain visible throughout the interaction and not disappear automatically.	Fixed footer or static banner during entire session.
Machine-Readability	Labels should be implemented in a structured, machine-readable format to ensure traceability and interoperability.	HTML meta tag <meta name="AI-content" content="true"> or IPTC/XMP field ai-generated=true.
Accessibility	Labels must be perceivable by all users, including those with visual or auditory impairments.	ARIA label or screen reader output: "AI-generated response" / "AI-generated content."

Practical Tip:

Transparency and labeling should be integrated during the design phase, not added later as a legal patch.

© A4Q Copyright 2025

UX and legal teams should jointly develop an internal labeling pattern set (e.g., standardized buttons, labels, or banners) to ensure consistency and compliance.

8.4 Organizational Implementation in Companies

Compliance with the transparency obligations under Article 52 of the EU AI Act requires not only technical but also organizational measures.
Companies should establish clear responsibilities, standardized procedures, and traceable documentation to ensure legally compliant and consistent labeling.

Recommended Implementation Steps:

1. **Inventory of AI Systems**
   Identify all systems that interact with users or generate media content (e.g., chatbots, voice assistants, generative tools).
   Objective: Maintain a complete overview to systematically assign transparency obligations.

2. **Risk Assessment**
   Analyze each system to determine whether it poses a **risk of deception, trust erosion, or violation of fundamental rights**.
   This evaluation forms the basis for classification as a **limited-risk** or **high-risk** system under **Article 6** of the AI Act.

3. **Labeling Policy**
   Develop internal standards for text, color, and metadata labels to ensure **uniform and verifiable labeling**.
   This policy should be part of the **UX design system** or **corporate design guidelines**.

4. **Approval Process**
   AI-driven applications or content may only be released **after review** by the responsible **compliance department** or **AI Compliance Officer**.
   The approval process ensures that all transparency disclosures are complete and correctly implemented.

5. **Audit and Documentation Evidence**
   Collect evidence of compliance with transparency obligations – e.g., **UI screenshots, technical documentation, log files, and version histories**.
   These records form an **audit trail** and enable verifiable compliance reviews.

6. **Training and Awareness**
   Provide regular training for **designers, developers, and marketing teams** on transparency requirements under Article 52.

© A4Q Copyright 2025

The goal is to build a **shared understanding** of legal duties, UX accountability, and documentation obligations.

8.5 Typical Errors and Compliance Risks

In practice, recurring issues often arise when implementing transparency requirements.
The following overview shows common risks, their impacts, and recommended mitigation measures to ensure compliance with Article 52.

Risk	Description	Recommended Mitigation Measure
Missing Labeling	Users cannot recognize that they are interacting with an AI system.	Provide clear, permanent UI indicators (e.g., “AI Response” label) or audio cues in voice systems.
Unclear Wording	Disclosures use vague, technical, or legalistic language and are not understood.	Conduct a UX review to ensure clarity and cultural neutrality of phrasing.
Missing Metadata	Content is visually labeled but not machine-readable.	Integrate labeling into metadata (e.g., IPTC/XMP, JSON-LD, or HTML meta tag).
Incomplete Logging	Implementation of transparency obligations cannot be verified during an audit.	Use logging systems with timestamps, hash values, and version control for tamper-proof documentation.
Emotion Recognition without Disclosure	The system analyzes emotions or biometric data without prior user notification.	Provide clear pre-information and explicit consent in accordance with Art. 52(2) and GDPR requirements.

8.6 Case Study: Labeling of Generative Content in Marketing

A mid-sized company uses a Large Language Model (LLM) to automatically generate product descriptions for its online store.
After editorial review, the texts are published directly on the website.

Error:
Publication occurs without disclosure that the content was AI-generated.
As a result, customers may believe the texts were fully written by humans.

© A4Q Copyright 2025

This violates Article 52(1) of the EU AI Act, as users are not informed that they are consuming AI-generated content.

Corrective Measures:

To ensure legal compliance and strengthen customer trust, the company implemented the following steps:

1. **Visible Footer Disclosure:**
   Each automatically generated text now includes the statement:
   "This text was created with the help of artificial intelligence."
   → Users clearly recognize that AI contributed to the creation process.

2. **Machine-Readable Labeling in Source Code:**
   The website's metadata now includes a tag that technically confirms AI generation:
   <meta name="ai-generated" content="true">
   → This supports transparent processing and future audits or automated detection systems.

3. **Internal Documentation Register:**
   Each AI-generated content item is recorded in a documentation register, including the date, system version, responsible person, and compliance review record.
   → This ensures traceability and verifiable evidence during audits.

Result:

By implementing these measures, the company complies with Article 52(1) of the EU AI Act and enhances trust and credibility among customers.
The documented labeling process creates a clear audit trail and strengthens legal certainty when using generative AI in marketing.

8.7 Practical Recommendations

Compliance with the transparency obligations under Article 52 requires both organizational and design-related actions.
Beyond legal conformity, the objective is to build user trust through visible accountability and responsible AI communication.

Recommended Best Practices:

1. **Develop an "AI Transparency Labeling Guide"**
   Integrate clear rules for labeling AI interactions and AI-generated content into your existing UX and corporate design system.
   The guide should include text templates, color standards, placement rules, and metadata formats (e.g., watermarks or metatags).
   → Ensures consistent and verifiable labeling across all applications.

© A4Q Copyright 2025

2. **Regular Technical and Functional Testing**
   Periodically verify that transparency labels are technically correct and perceivable.
   Use A/B testing, accessibility checks, and user feedback to ensure clarity, visibility, and accessibility.

3. **Conduct Periodic Transparency Audits**
   Evaluate new or modified AI applications, marketing campaigns, and voice bots for compliance with labeling and disclosure obligations.
   Document results in audit reports and implement corrective actions where necessary.

4. **Open Communication and Trust Building**
   Communicate transparently about your organization's use of AI—both internally and externally.
   Openness toward customers, employees, and regulators demonstrates accountability and strengthens trust in AI-driven systems.

© A4Q Copyright 2025

9 General Purpose AI (GPAI) & Systemic Risk

⏱ **Instruction Time:** 75 minutes

🎯 **Business Outcomes (BOs)**

- **BO 9.1:** Participants understand the significance of General Purpose AI (GPAI) within the framework of the EU AI Act and can identify the main obligations of providers under Articles 53–55, evaluating their relevance for user organizations.
- **BO 9.2:** Participants are able to assess the use of external GPAI models (e.g., LLMs, generative systems) in their own organizational context with respect to transparency, risk, and compliance, and derive practical recommendations for action.

Learning Objectives (LOs)

- **LO 9.1 (K1):** Participants can explain the term *General Purpose AI (GPAI)* and distinguish between foundation models and application-specific AI systems.
- **LO 9.2 (K2):** Participants can describe the core obligations of GPAI providers under Articles 53–55 of the EU AI Act and their intended purpose.
- **LO 9.3 (K2):** Participants can explain the relevance of these obligations for user organizations, particularly concerning transparency, risk, and liability.
- **LO 9.4 (K3):** Participants can conduct a compliance review for external GPAI models within their organization and formulate appropriate recommendations (e.g., contract review, transparency check, monitoring).
- **LO 9.5 (K1):** Participants know the regulatory framework for General Purpose AI models and understand their role in the European AI single market.

Key Terms:
General Purpose AI (GPAI), systemic risk, frontier model, AI model card, red-team testing, model governance, provider obligations, open-source models, downstream integration, technical documentation, transparency report, incident reporting.

Introduction: From LLMs to General Purpose AI

General Purpose AI (GPAI) – often referred to as foundation models – form the basis of many modern AI applications.
Unlike task-specific systems, they are designed for broad, adaptable use and can be fine-tuned for multiple downstream purposes such as text, image, or code generation, analysis, simulation, or decision support.

© A4Q Copyright 2025

Examples: GPT-4/5 (OpenAI), Claude (Anthropic), Gemini (Google), LLaMA (Meta), Mistral AI.

Their influence extends from chatbots and knowledge systems to governmental, educational, and enterprise applications.

→ For compliance professionals, this introduces a new dimension of risk:
Even if an organization does not develop its own model, it can still become liable as a deployer or downstream provider when integrating or using external GPAI systems.

9.1 Legal Framework: Articles 53–55 of the EU AI Act

Articles 53 to 55 of the EU AI Act define specific requirements for General Purpose AI (GPAI) – foundation models that can be used or repurposed for a wide variety of applications.
These provisions establish transparency, accountability, and technical traceability – both for providers and for user organizations that integrate or deploy such models.

Article	Key Provisions	Relevance for User Organizations
Art. 53	Obligations for GPAI providers – transparency, technical documentation, disclosure of training data sources, regular evaluations, and safety and robustness testing.	Establishes the foundation of trust in base models; serves as a key selection and procurement criterion for organizations.
Art. 54	*Systemic-risk models* – additional obligations for models with significant influence, scale, or market dominance, including risk analysis and safety assessments.	Relevant for organizations using or building upon market-leading models; enables informed risk assessments.
Art. 55	*Code of Practice* – encourages industry self-regulation and standardization through voluntary best-practice guidelines (e.g., model cards, red-team testing, data provenance reports, evaluation procedures).	Practical guidance for due diligence, procurement, and internal compliance processes.

The EU AI Act distinguishes between:

- **GPAI Providers** – developers or operators of base models (e.g., OpenAI, Anthropic, Google, Meta), and
- **Downstream Users or Integrators** – organizations that use these models via APIs, platforms, or embedded systems.

© A4Q Copyright 2025

User organizations must ensure that:

- the models they use comply with Articles 53–55,
- risk assessments and documentation are performed and kept up to date, and
- transparency and safety information provided by the model supplier is integrated into their own technical documentation and governance processes.

9.2 Obligations of GPAI Providers

Providers of General Purpose AI (GPAI) bear a heightened responsibility for the transparency, safety, and traceability of their foundation models.
The EU AI Act requires them to demonstrate – through technical, organizational, and documentary evidence – that their models are secure, reliable, and accountable.

Obligation Area	Description	Examples of Evidence
Technical Documentation	Detailed description of system architecture, training methods, data sources, and evaluation/testing procedures. Ensures traceability of model design, function, and limitations.	Model Card, architecture documentation, technical specifications
Transparency Report	Disclosure of data types, filtering mechanisms, and known limitations. Intended to inform regulators, partners, and user organizations.	Transparency Report, Data Summary, public provider report
Evaluation & Red-Team Testing	Regular testing for misuse potential, bias, hallucinations, and security vulnerabilities. Results must be documented and used for model improvement.	Testing reports, penetration tests, bias analyses, red-team assessments
Copyright Compliance	Evidence of lawful use of copyrighted material in training, including licenses, exceptions, or fair-use documentation.	License documentation, copyright declarations, legal assessments
Systemic Risk Assessment	Evaluation of whether the model's scale, reach, or influence poses systemic risks to society, security, or democratic processes.	Internal risk statements, external impact assessments

© A4Q Copyright 2025

Obligation Area	Description	Examples of Evidence
Code of Practice	Voluntary adherence to industry codes (e.g., EU Model Cards initiative, sectoral codes of conduct). Acts as proof of responsible practice.	Adherence statement, membership certification, participation records

These obligations primarily apply to GPAI providers, but they also serve as a reference framework for user organizations that rely on such models.
Organizations should verify that their suppliers comply with these obligations and provide verifiable documentation as part of their compliance or procurement process.

Guidance for User Organizations

Even though the primary obligations under Articles 53–55 fall on GPAI providers, companies using or integrating such models also have concrete responsibilities:

- **Contractual Safeguards:**
  Require suppliers to provide transparency reports, licensing evidence, and red-team testing documentation.
- **Documentation Obligation:**
  Integrate received evidence (e.g., model cards, evaluation reports) into the organization's own technical documentation.
- **Risk Assessment:**
  Evaluate whether the base models in use could pose **systemic**, **ethical**, or **security-related** risks for the company or its customers.
- **Procurement Policy:**
  Use the requirements of Articles 53–55 as **mandatory selection criteria** when acquiring or integrating third-party AI models.
- **Transparency Toward Third Parties:**
  Disclose internally and externally which GPAI models form the basis of your deployed AI systems.

9.3 Systemic Risks & Governance

Systemic risks arise when foundation models (General Purpose AI – GPAI) are deployed at scale across critical infrastructures, media ecosystems, administrative systems, or public services.
Because these models often form the basis for numerous downstream applications, they can have wide-reaching effects on security, transparency, and societal stability.

© A4Q Copyright 2025

Typical Forms of Systemic Risk:

- **Concentration Risk:** Dependence on a few global GPAI providers leads to technological and economic dependency.
- **Lack of Data Transparency:** Missing or incomplete disclosure of training data hinders the assessment of bias, fairness, and copyright compliance.
- **Cascading Errors:** Flaws in a base model can propagate through derived applications, resulting in widespread inaccuracies or failures.
- **Uncertainty over Data Provenance and Copyright:** Insufficient information on data origin creates legal exposure and reputational damage.

Responsibilities of User Organizations

Organizations that use or integrate GPAI models must ensure that they:

- use only compliant and verified GPAI models whose providers fulfill the requirements of Articles 53–55 of the EU AI Act,
- perform independent risk assessments, testing, and documentation—particularly regarding bias, robustness, and intellectual property,
- establish clear governance responsibilities (roles, approval workflows, escalation paths),
- implement monitoring and audit processes to identify new or escalating risks early,
- regularly assess dependencies on individual providers and develop diversification strategies where necessary.

Recommended Actions for Companies

1. **Establish a GPAI Risk Register:**
   Document all deployed foundation models, their versions, application contexts, and known limitations.
2. **Conduct Red-Team Tests and Prompt Audits:**
   Regularly test how models respond to prohibited, sensitive, or adversarial prompts.
3. **Integrate into Enterprise Risk Management:**
   Align AI risks with existing frameworks for risk, privacy, and compliance management.
4. **Supplier Selection Based on Compliance:**
   Include transparency reports, model cards, and Codes of Practice as procurement requirements.
5. **Training & Awareness Programs:**
   Educate employees on systemic risks and responsible GPAI usage.

© A4Q Copyright 2025

6. **Early Warning & Incident Response Processes:**
   Detect and report anomalies (e.g., unexpected outputs or data leaks) through structured incident management within the AI governance framework.

Conclusion:
Systemic risks extend beyond technology—they encompass strategic and organizational decisions.
A structured AI governance system, integrating GPAI risk management, compliance, and continuous monitoring, is essential for a trustworthy and sustainable use of General Purpose AI in enterprises.

9.4 Compliance Review of External GPAI Models (Checklist)

Even if a company does not develop its own foundation models, it remains responsible for the selection and deployment of external General Purpose AI (GPAI) systems.
A structured compliance review helps identify and mitigate legal and reputational risks at an early stage.
The following checklist supports organizations in assessing external GPAI models with regard to transparency, security, and regulatory compliance.

Review Area	Key Questions	Recommended Evidence
Contract & Licensing	Is the provider EU-compliant, certified, or registered? Does the contract include specific clauses covering obligations under Articles 53 ff. (e.g., transparency, documentation, safety checks)?	Service Level Agreement (SLA), Data Processing Agreement (DPA), compliance certificates, provider self-declaration
Transparency	Are the training data, sources, filtering mechanisms, and known limitations properly documented?	Model Card, Transparency Report, public provider disclosures
Bias & Security	Are evaluation reports, red-team tests, or independent audits available that identify bias, misuse potential, or vulnerabilities?	Testing reports, audit summaries, red-team documentation
Copyright	Is there a risk that copyrighted material was used during training? Have licenses or legal assessments been provided?	Legal review, provider statements, license documentation
Purpose of Use	How is the model used in your organizational context (e.g., text or image generation, data	Use case description, data-flow diagrams, internal approval logs

© A4Q Copyright 2025

Review Area	Key Questions	Recommended Evidence
	analytics, decision support)? Does this align with the model's intended purpose?	
Monitoring	Is the model's ongoing operation continuously monitored? Are there processes for incident detection and assessment of unexpected model behavior?	KPI dashboards, incident logs, monitoring reports

Recommended Implementation Approach

1. **Before Integration:**
   Conduct a pre-implementation compliance review using this checklist, and record all findings in the AI risk register.
2. **During Operation:**
   Establish continuous monitoring and periodically review provider documentation for updates.
3. **After Major Model Updates:**
   Reassess transparency, safety, and liability implications following significant model revisions.
4. **Documentation and Evidence:**
   Store all assessments and supporting evidence in a version-controlled compliance or quality management system.

9.5 Practical Example: Using an LLM in Customer Service

Initial Situation:
A company deploys a commercial Large Language Model (LLM) to automatically respond to customer inquiries in its online support system.
The AI generates text answers in real time, which are published directly on the company's website.

Issue:
Responses are automatically displayed without any indication that they were machine-generated and without a prior quality review.
This creates a risk of misleading users and publishing incorrect or inappropriate content.

Corrective Measures

© A4Q Copyright 2025

- **Labeling:**
  All automatically generated responses are now accompanied by the disclaimer:
  "This answer was generated using Artificial Intelligence."
- **Internal Review Process:**
  Each generated response undergoes editorial review and approval before publication.
- **Documentation:**
  An **audit trail** is implemented to log the model version, prompt used, reviewer, and approval date.
- **Model Verification:**
  The company reviews the GPAI provider's transparency documentation, including model cards, evaluation reports, and red-team test results.

Result

Through these measures, compliance is ensured with:
• **Article 53** – Transparency obligations for GPAI providers,
• **Article 52** – Labeling and disclosure requirements for AI-generated content, and
• **Article 55** – Adherence to an industry *Code of Practice*.

9.6 Recommendations for User Organizations

The deployment of General Purpose AI (GPAI) requires an integrated approach that combines legal, technical, and organizational dimensions.
User organizations must not only understand provider obligations but also embed them into their own AI governance and compliance systems.
The following recommendations outline how to operationalize these requirements effectively:

1. **Establish a GPAI Due-Diligence Process**
   Conduct a structured pre-assessment for each external model. Review documentation, transparency reports, licensing terms, and safety certifications before integrating the model into operational workflows.
2. **Implement Contractual Safeguards**
   Include specific compliance clauses in supplier and service contracts referencing Articles 53–55 of the EU AI Act, such as obligations to provide model cards, risk analyses, and red-team testing results.
3. **Embed Transparency and Monitoring into Governance Policies**
   Define internal procedures for oversight, continuous evaluation, and periodic reassessment of all deployed GPAI models as part of the AI governance or risk management system.

© A4Q Copyright 2025

4. **Maintain an AI Register**
   Record all GPAI models used within the organization, including details on provider, version, intended purpose, licensing status, known limitations, and testing results.
   This register serves as a compliance and audit reference for both internal and external reviews.

5. **Promote Training and Awareness**
   Regularly train employees on the opportunities and risks of generative AI, emphasizing the importance of transparency, accountability, and quality assurance in working with GPAI systems.

6. **Expand Incident Management**
   Integrate AI-related incidents into existing reporting processes.
   Systematically capture and analyze faulty outputs, data breaches, copyright issues, and abnormal model behavior.

7. **Adopt Red-Team Testing as a Best Practice**
   Conduct regular red-team tests – even for non–high-risk applications – to proactively identify vulnerabilities, bias, and manipulation risks.
   Document findings and remediation actions in the AI Risk Register.

© A4Q Copyright 2025

10 Fundamental Rights Impact Assessment (FRIA, Art. 27 EU AI Act)

⏱ **Recommended Duration:** 45 minutes

🎯 **Business Outcomes (BOs)**

- **BO 10.1:** Participants are prepared to structure a FRIA and integrate it into decision-making processes.
- **BO 10.2:** Participants are able to connect FRIA with Data Protection Impact Assessments (DPIA/DSFA) and leverage synergies between them.

Learning Objectives (LOs)

- **LO 10.1 (K1):** Participants know the purpose of a FRIA and understand its role as a core instrument for assessing fundamental rights risks.
- **LO 10.2 (K2):** Participants can explain which fundamental rights are typically affected by AI systems (e.g., equality, data protection, freedom of occupation).
- **LO 10.3 (K2):** Participants understand how a FRIA can be organizationally integrated into existing governance or approval workflows.
- **LO 10.4 (K3):** Participants can perform a simplified FRIA using a practical example, evaluate risks, and propose appropriate mitigation measures.
- **LO 10.5 (K1):** Participants know the key steps of a FRIA – from identifying impacted fundamental rights to documenting assessment results.

Key Terms

FRIA (Fundamental Rights Impact Assessment), Fundamental Rights, Discrimination, Bias, Fairness, Severity Matrix, Mitigation Measures, Stakeholder Engagement, Transparency, Complaint Mechanism, DPIA Alignment, Art. 27 EU AI Act.

Introduction

The Fundamental Rights Impact Assessment (FRIA) is a new and central instrument introduced by the EU AI Act.
It requires public authorities and certain private operators to assess, *before deploying high-risk AI systems*, whether such systems could negatively affect the fundamental rights of individuals.

© A4Q Copyright 2025

The objective is to identify and mitigate potential adverse impacts on privacy, equality, participation, freedom of expression, or employment opportunities at an early stage.

A FRIA complements existing data protection and ethical reviews, serving as a bridge between legal compliance, ethical accountability, and technical governance.

10.1 Legal Basis and Scope of Application

According to Article 27 of the EU AI Act, deployers of high-risk AI systems must conduct a Fundamental Rights Impact Assessment (FRIA) before putting such systems into use if they:

- operate in the public interest, or
- make decisions that may affect the fundamental rights of natural persons.

Examples of affected application areas:

- Recruitment and HR systems – access to employment, equal treatment
- Credit and scoring applications – economic participation and non-discrimination
- Education and testing platforms – access to education
- Public services – social benefits, migration, and security

Private organizations may voluntarily conduct a FRIA whenever fundamental rights may be significantly impacted.
This is considered best practice and can strengthen audit readiness and compliance maturity under the AI Act.

10.2 Structure and Recommended Steps of a FRIA

A FRIA follows a standardized and documented assessment process.

Step	Objective	Typical Content / Methods
1. System Description	Achieve clarity about the purpose, functionality, and user groups	System overview, data flows, decision logic, affected population groups
2. Fundamental Rights Analysis	Identify potentially affected rights	Reference to the EU Charter of Fundamental Rights: dignity, data protection, equality, education, participation

© A4Q Copyright 2025

Step	Objective	Typical Content / Methods
3. Risk Identification	Analyze possible negative effects	Discrimination, exclusion, misclassification, surveillance, degree of interference
4. Risk Evaluation	Assess likelihood and severity	Matrix: low – medium – high; balance between expected benefit and potential harm
5. Mitigation Planning	Define countermeasures to reduce risks	Transparency measures, human oversight, fairness checks, feedback and redress mechanisms
6. Documentation & Approval	Ensure traceability and accountability	Justified decision on deployment or rejection; version control; approval by AI Officer or compliance committee

Every FRIA must be well-documented, periodically reviewed, and updated whenever the AI system undergoes relevant changes (Art. 27 (3) AI Act).

10.3 Relationship and Integration with the Data Protection Impact Assessment (DPIA)

While both FRIA and DPIA (Art. 35 GDPR) are preventive assessment tools, they differ in focus and scope:

Criterion	FRIA (Art. 27 AI Act)	DPIA (Art. 35 GDPR)
Purpose	Protection of fundamental rights as a whole	Protection of personal data
Trigger	Deployment of a high-risk AI system	Processing of sensitive data with high risk
Perspective	Societal/ethical	Data protection / legal
Outcome	Fundamental rights risk analysis + mitigation plan	Data protection report with technical and organizational safeguards
Integration	Part of the conformity assessment dossier	Component of the data protection management system

© A4Q Copyright 2025

Recommendation:

Integrate both processes to avoid redundancy.

A combined FRIA–DPIA matrix ensures consistency across risk analyses and simplifies audit procedures.

Example:

For an AI-based recruitment tool, the same risk analysis can simultaneously cover both discrimination risks (FRIA) and data protection concerns (DPIA), resulting in a unified and efficient compliance process.

10.4 Practical Implementation of a FRIA – Step-by-Step Approach

To ensure that a Fundamental Rights Impact Assessment (FRIA) is implemented effectively, transparently, and auditably within an organization, the following steps should be systematically carried out:

1. Define Responsibilities

What to do:

Appoint a responsible person or unit—ideally the AI Officer or Compliance Manager—to lead and ensure the quality of the FRIA process.

Objective:

Clear accountability prevents gaps in risk assessment and ensures traceability for internal and external audits.

Best practice tip:

Document role assignments in your AI governance policy (e.g., *"FRIA Responsible: Jane Doe, AI Compliance Officer"*).

2. Develop a FRIA Template

What to do:

Create a standardized assessment form with defined sections and guiding questions, such as:

• Which fundamental rights could be affected?

• Which groups of individuals are particularly vulnerable?

• What mitigation measures are planned?

Objective:

A consistent process that ensures quality and facilitates documentation.

Best practice tip:

Use a structured table format (e.g., Excel sheet or compliance tool) to record risk levels, probability, and mitigation actions.

© A4Q Copyright 2025

3. Train Relevant Departments

What to do:

Provide training for HR, IT, Data Science, and Legal teams to help them recognize fundamental rights risks and contribute actively to assessments.

Objective:

Ensure that all involved understand the implications of their work for individuals' rights.

Best practice tip:

Implement short e-learning modules (30–45 minutes) complemented by case studies from your organization.

4. Integrate FRIA into Governance Processes

What to do:

Embed the FRIA as a mandatory step within existing decision-making and approval workflows:

• **Project initiation:** Conduct a FRIA pre-assessment.

• **Go-live:** Require an approved FRIA before deployment.

• **System updates:** Mandatory FRIA review and update.

Objective:

Make FRIA part of the operational routine, not a one-time compliance task.

Best practice tip:

Link the FRIA process to IT change or project management systems (e.g., ticketing or approval workflows).

5. Coordinate with Data Protection

What to do:

Align FRIA findings with the Data Protection Impact Assessment (DPIA) to avoid duplication of work.

Objective:

Consistent risk assessments and a holistic protection of fundamental rights.

Best practice tip:

Conduct joint workshops between the Data Protection Officer and AI Officer to identify synergies and jointly evaluate risks.

6. Conduct Regular Reviews

What to do:

Review and update each FRIA whenever:

• significant system changes occur,

• new datasets or models are introduced, or

• legal or regulatory requirements change.

© A4Q Copyright 2025

Objective:

Ensure that risk assessments and mitigation measures remain current.

Best practice tip:

Plan an annual FRIA review in the compliance calendar and track revisions in a version control system.

7. Communicate Results

What to do:

Document or publish the key findings—internally or publicly—to foster transparency and trust.

Objective:

Enable accountability for employees, customers, regulators, and the public.

Best practice tip:

• Maintain a short summary in the AI register (system, risks, measures, status).

• Include highlights in sustainability or compliance reports.

Outcome

Organizations that implement these seven steps achieve:

• a structured and audit-proof FRIA,

• clear accountability and synergy with data protection processes, and

• demonstrable integration of fundamental rights protection into all AI projects.

10.5 Synergies with Existing Management Systems

The FRIA can be effectively integrated into existing governance frameworks:

• **ISO/IEC 42001** – AI Management System: aligns with AI risk and compliance processes.

• **ISO/IEC 23894** – AI Risk Management: integrates stakeholder impact evaluation.

• **ISO/IEC 27701** – Privacy Extension to ISO 27001: connects FRIA to privacy management.

This alignment creates a unified evidence structure and supports a presumption of conformity under Article 40 EU AI Act.

10.6 Example: FRIA in Practice

Scenario:

A city administration plans to use an AI system to automate the review of housing subsidy applications. The goal is to reduce processing time and improve consistency through standardized evaluation criteria.

Conducted FRIA – Key Findings:

© A4Q Copyright 2025

Assessment Area	Evaluation / Measure
Affected Fundamental Rights	Equality, data protection, right to housing
Identified Main Risks	Bias in historical training data; lack of explainability; insufficient appeal mechanism for applicants
Implemented Mitigation Measures	Independent fairness testing by an external auditor; publication of decision criteria on the citizen portal; establishment of an appeal process with human oversight
Assessment and Decision	Deployment approved under specific conditions. Annual re-evaluation of models, datasets, and fairness metrics is mandatory.

Conclusion:

This example demonstrates how a FRIA can be practically implemented: risks are identified early, mitigation actions are documented, and responsibilities are clearly defined.
The combination of technical validation, organizational control, and transparent communication strengthens both legal compliance and public trust.

The FRIA is therefore a key instrument for realizing the human-centric approach of the EU AI Act.
It enables organizations to proactively protect fundamental rights, identify and document risks, and demonstrate accountability.
When combined with DPIA, ethical guidelines, and AI management systems, the FRIA becomes the core element of responsible AI governance

© A4Q Copyright 2025

11 Post-Market Monitoring, Reporting & Market Surveillance

⏱ **Duration:** 60 minutes

🎯 **Business Outcomes**

- **BO 11.1:** Participants develop an understanding of post-market processes and are prepared to apply monitoring plans.
- **BO 11.2:** Participants are equipped to cooperate effectively with supervisory authorities and the European AI Office.

Learning Objectives (LOs)

- **LO 11.1 (K2):** Participants can explain the purpose and requirements of a post-market monitoring plan under Article 61 EU AI Act.
- **LO 11.2 (K2):** Participants can describe the market surveillance process, including reporting obligations for serious incidents.
- **LO 11.3 (K3):** Participants can design a basic monitoring concept for a high-risk AI system.
- **LO 11.4 (K1):** Participants can identify roles, communication channels, and obligations toward market surveillance authorities and the European AI Office.
- **LO 11.5 (K1):** Participants know the key tasks and reporting duties within post-market monitoring.

Key Terms

Post-Market Monitoring, Serious Incident, Incident Reporting, Article 23 AI Act, Authority Cooperation, Market Surveillance, Corrective Actions, Documentation Obligations, Error Culture, Monitoring Dashboard, Proof of Compliance, Audit Follow-up.

Introduction

A provider's responsibility does not end once an AI system is placed on the market.
Under the EU AI Act, continuous post-market monitoring (PMM) is required to ensure that the system continues to comply with regulatory requirements and does not introduce new risks over time.

Post-market monitoring serves several purposes:

- **Detect** potential malfunctions or biases that appear during real-world use.
- **Evaluate** the effectiveness of risk management and oversight mechanisms.

© A4Q Copyright 2025

- **React** to emerging safety or compliance issues through documented corrective actions.

This section explains how organizations can plan and implement a compliant monitoring process and cooperate effectively with supervisory authorities and the European AI Office.

11.1 Obligations After Market Placement (Article 61 EU AI Act)

A provider's responsibility does not end once a high-risk AI system is placed on the market.
On the contrary, the EU AI Act explicitly requires organizations to ensure that the system remains safe, lawful, and effective throughout its entire lifecycle.

Article 61 EU AI Act mandates that providers of high-risk AI systems establish a structured and traceable Post-Market Monitoring System (PMM).
This system continuously verifies that the AI remains compliant with regulatory, technical, and ethical standards during operation.

According to Article 61(1) EU AI Act, providers must in particular:

1. **Establish a post-market monitoring system:**
   A defined process must be implemented to monitor system performance, behavioral deviations, and key metrics.
   The PMM must be integrated into the organization's governance structure and operate continuously, not sporadically.
2. **Systematically collect data on performance and malfunctions:**
   Relevant operational data must be gathered to assess reliability, accuracy, robustness, fairness, and stability – including technical logs, user feedback, complaints, and automated error reports.
3. **Analyze deviations from the conformity state:**
   Any change suggesting that the system no longer meets approved specifications must be investigated immediately.
   This includes performance degradation, model drift, emerging bias effects, or behavioral changes due to new data.
4. **Implement corrective measures or recalls:**
   If monitoring detects a risk to safety, fairness, or fundamental rights, immediate action is required – from software updates and retraining to temporary suspension or full withdrawal of the system.

The monitoring plan is a mandatory component of the technical documentation under Article 11 EU AI Act and must be prepared before market placement.
It forms the foundation of ongoing market surveillance and serves as proof that the provider fulfills its due diligence and monitoring obligations during operation.

© A4Q Copyright 2025

11.2 Objectives of Post-Market Monitoring

The purpose of post-market monitoring is to ensure the long-term safety, quality, and compliance of AI systems.
It bridges the gap between development and operation, supporting both technical stability and organizational accountability.

Key objectives include:

- **Ensuring continuous compliance:**
  Confirming that the system remains compliant with the EU AI Act, CE conformity declaration, and internal policies even after updates or prolonged use.
- **Detecting unexpected risks and bias effects:**
  Identifying deviations, biases, or discriminatory outcomes in real-world operations that were not evident in testing.
- **Evaluating performance and robustness over time:**
  Monitoring key performance indicators (KPIs) – such as accuracy, error rates, response times, or fairness metrics – to detect quality drift (model drift) early.
- **Providing traceability and accountability:**
  Supplying verifiable evidence for internal audits, external assessors, and supervisory authorities. Logs and reports form the basis for submissions to the **AI Office** or national oversight bodies.
- **Supporting re-evaluation or re-certification:**
  Monitoring outcomes informs periodic reviews of risk classification and re-certification when system functionality or data sources change.

Overall, post-market monitoring ensures that AI systems remain trustworthy, safe, and compliant – not only at launch but throughout their operational life.

11.3 Contents of a Monitoring Plan

An effective monitoring plan translates legal requirements into a structured corporate procedure.
It specifies what is monitored, how data is collected and evaluated, who is responsible, and what actions are taken when anomalies occur.

© A4Q Copyright 2025

Section	Description
Objectives & Scope	Define which aspects of performance and quality are monitored (accuracy, fairness, safety, user feedback, stability). The scope must cover all relevant components, including subsystems and data sources.
Indicators / KPIs	Establish measurable performance indicators such as error rates, false positive ratios, performance drift, frequency of incidents, or fairness metrics.
Data Sources	Identify monitoring data sources: system logs, user complaints, audit reports, support tickets, external data feeds, or statistical evaluations.
Roles & Responsibilities	Assign accountability: AI Officer (overall responsibility), domain experts (quality evaluation), compliance officers (reporting coordination), IT monitoring team (technical data collection).
Reporting Cycles	Define reporting frequency – e.g., monthly reviews for operations, quarterly management reports, annual compliance submissions to authorities.
Escalation Paths	Define thresholds and decision-making procedures: When does an event qualify as an incident? Who authorizes shutdowns or notifications to authorities?

Example Indicators for Post-Market Monitoring:

- System performance deviation exceeding 10% from baseline.
- Three or more incidents within 30 days.
- Noticeably higher error rates for specific user groups → trigger a fairness audit.

Best Practice Recommendation:
Monitoring plans should be linked to other governance tools – such as the risk register, incident management process, and quality management system (QMS).
This creates an end-to-end traceability chain connecting risk assessment, system operation, and continuous improvement.

11.4 Serious-Incident-Reporting (Art. 62 EU AI Act)

A “Serious Incident” is defined under Article 62 EU AI Act as *any event related to the behavior of an AI system that results in, or is likely to result in, harm to the rights, safety, or integrity of persons.*

© A4Q Copyright 2025

This includes any situation where an AI system's operation causes, contributes to, or amplifies a safety risk or violation of fundamental rights.

A serious incident typically occurs when the system's behavior leads to:

- **Violations of fundamental rights** (e.g., discrimination, unlawful rejection of applications, lack of recourse or appeal),
- **Significant safety risks** to individuals, systems, or critical infrastructures, or
- **Unforeseen malfunctions** with potential harmful consequences (e.g., false medical diagnoses, automated misclassifications).

This definition encompasses both technical malfunctions and legally or ethically relevant misjudgments – regardless of whether actual harm has occurred or merely a high likelihood exists.

Obligations Upon a Serious Incident (EU-Wide Requirements)

Under the EU AI Act, both providers and deployers of high-risk AI systems must act immediately when a serious incident occurs.
These duties are harmonized across the EU to ensure swift, transparent, and coordinated responses aimed at protecting public safety, fundamental rights, and societal trust.

1. Notification Within 15 Calendar Days

The provider must report the incident to the relevant national market surveillance authority within 15 days of becoming aware of it.
This obligation applies even if no harm has yet occurred, but a substantial likelihood exists.

The report must include all available information at the time of detection:

- System ID and affected modules
- Nature of the malfunction or behavior
- Potential impacts and scope
- Preliminary corrective actions taken

The 15-day period starts from the first internal awareness of the incident, not from its final analysis.

Deployers are likewise required to immediately inform their provider, enabling the provider to submit the report on time.

Examples of National Authorities:

© A4Q Copyright 2025

Country	Market Surveillance Authority	Data Protection Authority
Austria	Federal Ministry for Climate Action (BMK)	Data Protection Authority (DSB)
Germany	Federal Network Agency (BNetzA)	Federal Data Protection Commissioner (BfDI)
France	DGCCRF	CNIL
Italy	Ministry of Enterprises and Made in Italy (MIMIT)	Garante per la Protezione dei Dati Personali
Spain	MINECO	AEPD
Netherlands	Authority for Consumers & Markets (ACM)	Autoriteit Persoonsgegevens (AP)
Belgium	SPF Économie	Autorité de Protection des Données (APD)
Sweden	Konsumentverket	Integritetsskyddsmyndigheten (IMY)

Each national authority must forward the report to the EU AI Office, which coordinates a union-wide evaluation.

2. Parallel Notification to the EU AI Office

In addition to national reporting, the provider must also inform the AI Office of the European Commission.

- The AI Office acts as a central coordination body and maintains a European incident database.
- For systemic risks (e.g., widespread flaws in GPAI or foundation models), the AI Office may initiate EU-level investigations or immediate measures.
- Reporting will be facilitated through a unified “AI Incident Reporting Portal” once operational.

3. Submission of an Initial Analysis and Planned Actions

The initial report must include:

- A concise technical description of the incident,
- Date, location, and affected system versions,
- Nature and severity of the risk,
- Estimated number and type of impacted individuals or systems,

© A4Q Copyright 2025

- Initial mitigation steps and containment measures.

This preliminary information enables authorities to assess risk severity and, if necessary, trigger urgent responses, such as user warnings or system recalls.

4. Submission of a Final Report After Remediation or Update

Once corrective actions are completed or the system is updated, a final report must be submitted containing:

- A root-cause analysis,
- A detailed list of corrective and preventive actions,
- Evidence of effectiveness (e.g., test or validation results),
- Reactivation date of the system (if applicable).

The final report is sent to the same authorities that received the initial notification.
Increasingly, coordination will occur digitally through the EU Market Surveillance Platform, which standardizes communication between national regulators and the AI Office.

Purpose and Expected Outcome

The Article 62 reporting system aims to ensure early risk detection, transparent root-cause analysis, and EU-wide learning from incidents.
The multi-level reporting chain – from deployer → provider → national authority → AI Office – establishes a pan-European early warning mechanism that strengthens the safety, reliability, and accountability of AI systems.

Example:
An HR screening system exhibits significantly higher rejection rates for applicants over 50.
The AI Officer suspends the algorithm, initiates a bias audit, informs both the national market surveillance authority and the EU AI Office, and submits a final report after retraining, demonstrating corrected and validated results.

11.5 Cooperation with Market Surveillance Authorities and the EU AI Office

The EU AI Act establishes a multi-level market surveillance system based on cooperation, accountability, and transparency.
National authorities conduct oversight within their jurisdictions, in close coordination with the EU AI Office, which ensures consistent interpretation and implementation of the regulation across the European Union.

© A4Q Copyright 2025

Main responsibilities of market surveillance authorities:

- **Sampling inspections and audits:**
  National authorities regularly review registered high-risk systems. These inspections – announced or unannounced – may include examination of documentation, logging systems, models, and audit reports.
- **Coordination by the EU AI Office:**
  The AI Office acts as the central EU coordination body, developing common guidelines, conducting risk analyses, and facilitating information exchange among Member States.
  In severe cases, it may order joint investigations or convene technical expert groups.
- **Obligations of providers:**
  Companies must grant authorities **timely access** to all relevant materials – including technical documentation, audit logs, versioning evidence, and monitoring reports.

Recommended procedure for responding to authority inquiries:

1. **Establish a central contact point:**
   Appoint a designated liaison (e.g., AI Officer or Compliance Manager) to serve as the **single interface** for all communications with supervisory authorities.
2. **Provide standardized audit reports and model versions:**
   Maintain a clear documentation structure – such as an audit dossier, model changelog, and versioning tables – to ensure traceability and minimize review effort.
3. **Proactive communication on risks or changes:**
   Notify authorities in advance of significant modifications to models, datasets, or intended purposes, before re-certification becomes necessary.
4. **Document all regulatory interactions:**
   Record each inquiry, response, and inspection in an internal **Regulatory Interaction Log**, including date, contacts, topic, and outcome. These records serve as formal evidence of cooperative compliance during audits.

Practical note:
Authorities explicitly view open, fact-based collaboration with providers as a positive indicator of maturity and responsibility in corporate AI governance.

11.6 Best Practice: Continuous Risk Re-Evaluation

Post-market monitoring must be linked to an organization's ongoing risk re-evaluation process.
At least once per year, or whenever substantial system changes occur, companies should reassess the risk classification of their AI systems to confirm that the assigned category and safeguards remain appropriate.

© A4Q Copyright 2025

Typical triggers for re-evaluation:

- **Significant model modifications** (e.g., retraining, new data sources, altered weights or algorithms).
- **New application domains or target groups** (e.g., redeployment of an internal tool in a public-sector context).
- **Changes in legal or regulatory frameworks** (e.g., new AI Office guidelines or national implementing acts).

Documentation of results:
All findings must be recorded in the risk register and included in the annual post-market compliance report. If increased risk is identified, a renewed conformity assessment under Articles 17 ff. EU AI Act becomes mandatory.

Goal:
This continuous review process reinforces legal certainty and demonstrates that the organization takes its monitoring and due diligence obligations seriously.

11.7 Practical Example: Post-Market Monitoring and Regulatory Cooperation in Public Administration

Scenario:

A public employment agency deploys an AI system for the automated pre-screening of job applications. The model analyzes submitted CVs based on qualifications, keywords, and experience profiles, producing ranked shortlists for HR review.
Objective: to improve efficiency while maintaining fairness and transparency.

Post-market findings:

After several months of live operation, the required post-market monitoring (Art. 61 EU AI Act) reveals anomalies:

- The monitoring dashboard shows that applicants over 55 consistently receive lower scores than younger applicants with comparable qualifications.
- The AI Officer classifies the issue as a Serious Incident under Article 62 EU AI Act, reports it to the national market surveillance authority and the EU AI Office within the statutory timeframe.
- The system is temporarily suspended to prevent further disadvantage, pending an independent fairness audit by an external body.

© A4Q Copyright 2025

- Investigation confirms that the bias originated from historical training data in which older applicants were under-represented.

Corrective and preventive actions:

1. **Retraining with a revised dataset** including balanced age representation.
2. **Independent re-evaluation** confirming improved fairness and model robustness.
3. **Conditional re-deployment** under specific obligations:
    - Semi-annual monitoring reports with bias analyses.
    - Mandatory fairness tests before each model update.
    - Regular HR training on interpreting AI scores and maintaining human oversight.

Result:

After corrective action, the system is re-approved for use. Monitoring reports indicate stable, non-discriminatory performance.

The employment agency records the entire case in its conformity dossier under Article 11 EU AI Act.

Key takeaway:

This example illustrates how post-market monitoring, incident reporting, and regulatory cooperation are interlinked.

An active, well-documented culture of accountability and learning enables organizations to detect risks early, maintain compliance, and strengthen public and institutional trust in AI-driven decision-making.

© A4Q Copyright 2025

12 Governance, Organization & Roles within the Company

⏱ **Duration:** 45 minutes

🎯 **Business Outcomes:**

- **BO 12.1:** Participants are prepared to define and co-design roles and responsibilities within an AI governance framework.
- **BO 12.2:** Participants are able to establish internal training and policy programs that strengthen a culture of compliance.

Learning Objectives (LOs):

- **LO 12.1 (K2):** Participants can explain the key components of an AI governance structure and their importance for compliance and quality.
- **LO 12.2 (K3):** Participants can design responsibility structures, escalation paths, and committees within an AI governance model.
- **LO 12.3 (K2):** Participants can describe how training and awareness programs contribute to building a strong compliance culture.
- **LO 12.4 (K1):** Participants can identify key governance terms such as *policy*, *accountability*, and *AI Governance Committee*.
- **LO 12.5 (K1):** Participants know the core role distribution in AI governance, especially the tasks of the AI Officer, Compliance Board, and domain departments.

Key Terms:
AI Governance, Accountability, AI Officer, AI Governance Committee, Compliance Board, RACI Matrix, Roles & Responsibilities, Policy, Escalation Path, Awareness Program, Training Matrix, Art. 4(4) AI Act.

Introduction

AI governance refers to the organizational structures, processes, and roles that ensure artificial intelligence is used lawfully, safely, and ethically.
An effective governance system integrates the legal requirements of the EU AI Act, the GDPR, and ISO/IEC 42001 with internal accountability, training, and a culture of transparency.

12.1 Structure of an AI Governance System

A robust AI governance framework operates on three coordinated levels:

© A4Q Copyright 2025

Level	Objective	Typical Instruments
Strategic	Define direction, risk appetite, priorities	AI Governance Committee, executive reporting
Tactical	Manage implementation, allocate resources, maintain policies	Policies, RACI Matrix, role profiles
Operational	Execute processes, perform monitoring, maintain documentation	Audit protocols, incident management, training plans

Clear accountability assignment is crucial:
Every activity – e.g., fairness audits, logging, or retraining – must have a responsible role, an approval level, and a documented decision path.

12.2 Key Roles and Responsibilities

A well-functioning AI governance framework requires clearly defined roles, responsibilities, and reporting lines.
This ensures that regulatory obligations under the EU AI Act and internal quality and security standards are applied consistently.

Role	Main Responsibilities	Reporting Line
AI Compliance Officer	Coordinates all AI compliance activities; conducts risk assessments; ensures compliance with the EU AI Act; prepares internal and external audits.	To Executive Management / CISO
Conformity Manager	Maintains and updates the technical dossier; coordinates conformity assessments; acts as the primary contact for market surveillance authorities and certification bodies.	To AI Officer / Legal
Domain Expert	Ensures the data's relevance and quality; validates model outputs within the specific application domain; documents tests and modifications.	To the AI Committee
Ethics / Diversity Officer	Reviews fairness, equality, and societal impact; contributes to ethical impact assessments and bias evaluations.	To the AI Committee

© A4Q Copyright 2025

Role	Main Responsibilities	Reporting Line
IT Security & Data Protection	Ensures data protection and cybersecurity; oversees logging systems and access controls; coordinates with ISMS and GDPR officers.	To CISO / DPO

Together, these roles form the **organizational core of AI compliance**.
Clearly assigned responsibilities and reporting paths guarantee early risk detection, effective mitigation, and demonstrable accountability under Article 4(4) EU AI Act.

12.3 AI Governance Committee

An interdisciplinary AI Governance Committee (AI Committee) coordinates all activities related to AI risk management, governance, and compliance.
It serves as the central steering body for responsible AI use and ensures continuous alignment with the regulatory obligations of the EU AI Act.

Key tasks of the AI Committee:

- **Review of new AI use cases** before deployment: assess risk classification, identify fundamental-rights implications, and approve or escalate as needed.
- **Approval of policies, ethics guidelines, and audit plans:** ensure internal governance documents align with legal requirements and corporate goals.
- **Oversight of post-market monitoring reports:** review the effectiveness of risk-mitigation measures and analyze incident reports and monitoring outcomes.
- **Escalation management for serious incidents:** evaluate critical cases and coordinate communication with management, supervisory authorities, and external auditors.

Best practice:
The committee should be **interdisciplinary**, combining technical, legal, and ethical expertise.
Recommended participants include representatives from:

- Legal & Compliance
- Data Protection (DPO)
- IT / Cybersecurity (CISO)
- Human Resources (HR)
- Product Management

© A4Q Copyright 2025

- Ethics or Sustainability functions

The committee should meet regularly (e.g., quarterly) and document all decisions, actions, and recommendations in a Governance Register.
This approach promotes transparency, clear accountability, and verifiable compliance with Article 4(4) EU AI Act.

12.4 Internal Policies and Control Mechanisms

An effective AI governance framework relies on clear internal regulations and traceable control mechanisms.
These documents define how AI systems are developed, operated, monitored, and periodically reviewed, ensuring accountability, transparency, and legal certainty in line with the EU AI Act.

Key governance documents:

- **AI Policy:** Defines principles, responsibilities, and approval processes for the development, deployment, and oversight of AI systems.
- **Standard Operating Procedures (SOPs):** Detailed work instructions for specific processes such as incident handling, bias testing, model retraining, or post-market monitoring.
- **Compliance Register:** A record of all AI systems in use, including version, purpose, risk classification, responsible roles, and current audit status. This serves as evidence for internal and external audits.
- **Policy Cycle:** Regular (at least annual) review of all governance documents to ensure alignment with current regulations and to incorporate lessons learned from audits or incidents.

This structure enables organizations to establish consistent standards for AI use and systematically fulfill their accountability obligations under Articles 4(4) and 29 EU AI Act.

12.5 Training and Awareness Programs

A sustainable compliance culture depends not only on formal policies but also on qualified and aware employees. Training and awareness initiatives are key to embedding EU AI Act requirements in daily operations.

Recommended training and awareness components:

- **Foundational training:** Introduction to the EU AI Act principles, risk categories, key organizational roles, and typical compliance obligations.
- **Role-specific training:** Advanced sessions for departments such as HR, IT, development, or management, focusing on their respective responsibilities in AI operations.

© A4Q Copyright 2025

- **E-learning and certification:** Digital training modules with automatic reminders when legal or system changes occur, combined with completion certificates for audit evidence.
- **Workshops on error culture:** Promote a “learn-from-incidents” approach – analyzing real cases to strengthen prevention and transparency.
- **Awareness campaigns:** Ongoing communication through intranet, newsletters, posters, or short videos addressing topics such as *Responsible AI* or *Bias Awareness*.

Objective:
All employees should understand where and how AI is used, what risks exist, and how to respond or escalate concerns appropriately.

12.6 Interfaces with Existing Management Systems

Efficient AI governance should not operate in isolation.
By linking AI governance to established ISO-based management systems, organizations can avoid duplication and consolidate compliance evidence.

Management System	Connection to AI Governance
Information Security Management System (ISMS)	Ensures data protection and system integrity; supports security requirements under Art. 15 EU AI Act.
Quality Management System (QMS)	Maintains process documentation, version control, and audit readiness per Art. 17 EU AI Act.
Data Protection Management System (DPMS)	Integrates GDPR obligations, Data Protection Impact Assessments (DPIAs), and data subject rights.
Compliance Management System (CMS)	Coordinates risk management, escalation procedures, and audit planning as part of overall corporate compliance.

These interfaces strengthen organizational efficiency, consistency of evidence, and the integration of AI into existing audit and control processes.

12.7 Example – Governance Implementation in Practice

Scenario:
A public transport operator plans to implement an AI-based dynamic ticket-pricing system.
The goal is to adjust fares dynamically based on demand, time of day, and occupancy to distribute

© A4Q Copyright 2025

passenger loads more evenly.
The AI analyzes historical booking data, weather forecasts, event schedules, and real-time passenger volumes.

During the planning phase, the organization identifies that the system may process personal data (e.g., time and location profiles) and could thus pose regulatory risks under the EU AI Act and GDPR.
It classifies the project as a “High-Impact Use Case” and integrates it into its internal AI governance framework.

Implemented measures:

1. **Appointment of an AI Officer and establishment of a multidisciplinary Governance Board**
    - The AI Officer coordinates all compliance activities and reports directly to senior management.
    - The Governance Board includes representatives from Legal, Data Protection, IT Security, Operations, Communications, and Pricing.
    - The Board reviews all AI projects, issues approvals, and evaluates audit results.
2. **Definition of roles and responsibilities**
    - Monitoring Lead: Continuously observes pricing recommendations and detects anomalies.
    - Fairness Officer: Ensures no user group (e.g., students, seniors, commuters) is systematically disadvantaged.
    - Incident Manager: Executes immediate corrective actions for irregular results such as extreme fare deviations or customer complaints.
    - All roles are recorded and updated in the Compliance Register.
3. **Implementation of an AI Policy with transparency and feedback mechanisms**
    - All algorithmic pricing decisions must be explainable.
    - Requirements include:
        - Disclosure of the main factors influencing price calculation.
        - Customer portal notice: “Prices are partially determined using an AI system.”
        - Feedback channel for passengers to report unusual fare fluctuations.
    - Major system changes (e.g., new data sources) trigger a new risk assessment and Governance Board approval.
4. **Training and continuous qualification of staff**
    - Employees in pricing and customer service receive annual training on:
        - Fundamentals of the EU AI Act,

© A4Q Copyright 2025

        - Fairness and non-discrimination,
        - Handling customer feedback regarding AI-based decisions.
    - New employees must complete an e-learning module on the *Responsible AI Policy* before gaining system access.

5. **Regular audits and external evaluations**
    - Annual internal audits verify pricing logic and fairness metrics.
    - Every two years, an independent external audit tests bias control and system stability.
    - Results are documented and reported to the AI Governance Board along with action plans.

Outcome:
Through early integration into the AI governance framework, the company achieves a transparent and accountable structure:

- All decisions are traceable.
- Monitoring and audits are conducted regularly.
- Passenger feedback directly informs system improvements.

The supervisory authority classifies the approach as best practice:
The transport provider not only complies with the EU AI Act requirements (transparency, risk management, fairness) but also establishes a proactive governance culture that fosters trust among regulators and the public.

Key takeaway:
According to the EU AI Act, this example demonstrates that governance is not a bureaucratic burden – it's a "strategic enabler" of responsible, sustainable, and trustworthy AI deployment. Because nothing says "innovation" quite like another committee meeting, three new policies, and a 47-page audit trail.

© A4Q Copyright 2025

13 Minimal Risk & Voluntary Governance (“Ethical AI”)

⏱ **Duration:** 40 minutes

🎯 **Business Outcomes:**

- **BO 13.1:** Participants develop awareness of voluntary governance frameworks such as ISO/IEC 42001 and the OECD AI Principles.
- **BO 13.2:** Participants are prepared to connect ethical guidelines with CSR and ESG goals.

Learning Objectives (LOs)

- **LO 13.1 (K2):** Participants can describe voluntary international governance frameworks such as ISO/IEC 42001, the OECD AI Principles, and UNESCO Guidelines.
- **LO 13.2 (K2):** Participants can explain how voluntary governance measures complement legally binding requirements.
- **LO 13.3 (K3):** Participants can integrate ethical guidelines with CSR and ESG objectives into a holistic AI governance approach.
- **LO 13.4 (K2):** Participants can explain the value of Ethical Impact Assessments (EIA) for organizations.
- **LO 13.5 (K1):** Participants know the basic importance of voluntary governance instruments for building trust, self-regulation, and international interoperability.

Key Terms:
Ethical AI, Corporate Social Responsibility (CSR), Environmental Social Governance (ESG), OECD AI Principles, UNESCO Ethics Recommendation, ISO/IEC 42001 governance aspects, Ethical Impact Assessment (EIA), voluntary self-commitment, ethics guidelines, transparency culture.

Introduction

While the EU AI Act sets mandatory minimum standards, many organizations deliberately go beyond these obligations.
Voluntary governance frameworks – such as ISO/IEC 42001 (AI Management System Standard), the OECD Principles for Trustworthy AI, or the UNESCO Ethical Guidelines – create a structure for developing and deploying AI responsibly, sustainably, and in line with social values.

These frameworks not only support compliance but also strengthen corporate reputation, stakeholder trust, and the achievement of CSR (Corporate Social Responsibility) and ESG (Environmental, Social, Governance) objectives.

© A4Q Copyright 2025

13.1 Voluntary Governance under ISO/IEC 42001

The ISO/IEC 42001 standard defines an AI Management System (AIMS) similar to ISO 9001 (Quality Management) or ISO/IEC 27001 (Information Security Management).
It helps organizations manage AI-related risks in a structured way and clearly assign responsibilities – even for systems not covered by legal obligations ("minimal risk AI").

Core elements:

- AI policy and objectives for responsible AI use
- Defined roles and responsibilities (e.g., AI Governance Officer)
- Risk management aligned with **ISO/IEC 23894**
- Documentation, audits, and continuous improvement
- Stakeholder engagement and transparency obligations

Practical example:
A company uses a marketing AI that does not fall under the EU AI Act.
It voluntarily implements an AI Management System (AIMS), adopts an ethics policy, and conducts annual audits. Result: Greater customer and investor trust and an improved, documented risk profile.

13.2 OECD, UNESCO, and IEEE Guidelines for Trustworthy AI

International frameworks establish common ethical values that extend beyond legal compliance:

OECD Principles for Trustworthy AI (2019):

1. Inclusive growth, sustainable development, and well-being
2. Human-centered values and fairness
3. Transparency and explainability
4. Robustness, security, and safety
5. Accountability

UNESCO Recommendation on the Ethics of AI (2021):

- Human rights as the central guiding principle
- Prohibition of mass surveillance and social scoring
- Protection of cultural diversity and data sovereignty

IEEE *Ethically Aligned Design*:

© A4Q Copyright 2025

- Human well-being as the primary goal
- Accountability through explainability and auditability
- Transparency by default

Conclusion:
These frameworks foster global alignment of ethical standards and enhance the acceptance and trustworthiness of AI systems beyond legal boundaries.

13.3 Ethical Impact Assessment (EIA)

Similar to a Data Protection Impact Assessment (DPIA), a voluntary Ethical Impact Assessment (EIA) evaluates the societal, cultural, and environmental impacts of an AI system.

Typical evaluation criteria:

- Human dignity and autonomy
- Equality and diversity
- Transparency and accountability
- Environmental sustainability (energy use, resource consumption)

Practical example:
A city government introduces a citizen app for traffic management and uses an EIA to assess whether elderly people or those without smartphones might be disadvantaged.
Result: The system is adjusted to include analog access options and multilingual communication, ensuring inclusivity and equal participation.

13.4 Linking Ethics, CSR, and ESG

The integration of ethical AI governance with Corporate Social Responsibility (CSR) and Environmental, Social, and Governance (ESG) strategies is increasingly becoming a competitive advantage.

CSR perspective: Responsibility toward employees, customers, and society.
ESG perspective: Sustainability reporting that includes **AI ethics** as part of the **governance pillar**.

Example of integration:

ESG Area	AI Relevance	Possible Measure
E – Environment	Resource efficiency of AI infrastructure	Monitoring of energy consumption and CO_2 footprint
S – Social	Non-discrimination and inclusion	Fairness audits; diversity-aware training data

© A4Q Copyright 2025

ESG Area	AI Relevance	Possible Measure
G – Governance	Transparent decision-making processes	AI Ethics Board; public transparency report

Organizations that align ethics, CSR, and ESG benefit from stronger brand reputation, improved employee retention, and easier access to sustainable investments.

13.5 Scenario: Ethical AI at a Telecommunications Provider

Context: A telecommunications company develops an AI system for customer churn prediction.

Approach:

- Voluntary application of ISO/IEC 42001 to establish a governance framework
- Creation of an Ethics Board to review training data and model design
- Integration of ethical AI principles into ESG reporting
- Annual ethics audit conducted by the internal audit department

Result:

The system demonstrates no evidence of discriminatory patterns; accountability reports are made publicly available.

The company receives an industry award for “Responsible AI Leadership 2028.”

© A4Q Copyright 2025

14 Audit Readiness, Audit Trails & Sanctions

⏱ **Training duration:** 30 minutes

🎯 **Business Outcomes:**

- **BO 14.1:** Participants are prepared to systematically plan and conduct internal and external audits.
- **BO 14.2:** Participants are able to implement corrective and improvement measures based on audit findings.

Learning Objectives (LOs)

- **LO 14.1 (K2):** Participants can explain the purpose, process, and requirements of internal and external AI audits.
- **LO 14.2 (K3):** Participants can compile the necessary documentation, evidence, and audit checklists.
- **LO 14.3 (K2):** Participants can describe typical audit findings (nonconformities) and their regulatory significance.
- **LO 14.4 (K3):** Participants can derive appropriate corrective and continuous improvement actions from audit results.
- **LO 14.5 (K1):** Participants recall the key sanction framework of the EU AI Act (Art. 71).
- **LO 14.6 (K1):** Participants know the basic steps required to prepare for an AI audit.

Key Terms:

Audit readiness, audit policy, audit trail, self-audit, finding, corrective action, re-audit, audit interview, sanction framework, administrative fine, authority notification, documentation versioning, cross-audit learning.

Introduction: Why Audit Readiness Matters

Audits are a central control mechanism under the EU AI Act – ensuring traceability, legal certainty, and trust.
Organizations operating AI systems, especially high-risk applications, must at any time be able to prove that all regulatory obligations are met.

Audit readiness, therefore, means:

- Comprehensive and up-to-date documentation,
- Clearly defined responsibilities,

© A4Q Copyright 2025

- Practiced procedures for inspections and incident reporting.

A well-prepared audit process not only reduces the risk of fines and reputational damage but also strengthens internal quality management and learning processes.

14.1 Types of Audits and Responsibilities

Audit Type	Characteristics	Responsible Party
Internal Audit	Regular, self-initiated review of AI Act obligations (Art. 61)	AI Officer / Compliance Manager
External Audit (Third Party / Notified Body)	Independent review before market placement or after major system changes (High-Risk Systems)	Provider / Manufacturer
Regulatory Audit	Conducted by market surveillance authorities or the AI Office in case of suspicion or random sampling	National Supervisory Authority
Combined Audit (DPIA + AI Conformity)	Integrated review combining data protection and AI compliance	Data Protection Officer & AI Officer jointly

14.2 Audit Preparation

Before any audit, the following evidence must be available:

1. **Technical documentation** (Art. 11 AI Act): current, complete, and traceable.
2. **Risk management records** (Art. 9): identified risks, evaluations, mitigation actions, review cycles.
3. **Human oversight documentation** (Art. 14): training materials and authorization protocols.
4. **Logging and audit trail reports** (Art. 12, 23): complete, timestamped logs.
5. **Post-market monitoring reports** (Art. 24): ongoing performance and safety data.
6. **Training and governance evidence** (Art. 4(4), 29): roles, attendance records, learning verification.
7. **Incident management records** (Art. 23): reports, analyses, mitigation measures.
8. **Declaration of conformity and CE documentation** (Art. 19, 49): valid certificates and EU database entries.

© A4Q Copyright 2025

Practical tip: Maintain an *"Audit Readiness Register"* in your GRC or SharePoint system to consolidate and version all required evidence.

Audit Trails and Evidence Chains

An audit trail is the traceable sequence of records showing how and when an organization fulfilled its obligations under the EU AI Act.
It allows auditors to reconstruct decisions, changes, and actions – both technically and organizationally.

Purpose and Benefits

- Ensures traceability under Art. 12, 23, 61 AI Act
- Provides proof for *Presumption of Conformity* (Art. 40)
- Enables transparency for regulators and internal auditors
- Forms the basis for improvement tracking and liability defense

Structure of a Complete Audit Trail

Phase	Content / Evidence	Typical Source
1. **Design Phase**	System description, purpose definition, risk classification, FRIA/DPIA results	Project files, FRIA report
2. **Training Phase**	Data sources, data quality checks, bias test protocols, model versions	Data Governance Register
3. **Validation Phase**	Test results, accuracy/fairness metrics, approval protocols	Validation report
4. **Deployment Phase**	CE Declaration, EU Database registration, training records	Compliance Dossier
5. **Operational Monitoring**	Logs, dashboards, incident reports, human intervention logs	Monitoring System
6. **Audit Phase**	Audit reports, findings, corrective action plans	Audit Register
7. **Improvement Phase**	Evidence of corrective actions, re-evaluations, lessons learned	Management Review

© A4Q Copyright 2025

Technical Requirements

- **Chronological documentation:** every change or decision must include a timestamp and the responsible person.
- **Immutability:** use tamper-proof storage (e.g., WORM, blockchain hash, digital signatures).
- **Version control:** every model or policy version must have a unique identifier (e.g., AI-System v1.03 – Audit 2025-05).
- **Metadata linkage:** connect evidence to the relevant EU AI Act obligations (Art. 9–24).
- **Access control:** only authorized personnel (AI Officer, Compliance, Auditors) may modify or view data.

Example: Audit Trail of an HR Screening System

1. **Risk classification:** High-Risk under Annex III – record dated 02 Mar 2025
2. **Dataset review:** Bias Report #HR-2025-07, DIR = 0.88
3. **Model validation:** Fairness Audit on 17 Apr 2025, approved by AI Officer
4. **Training:** HR Training #2025-06 – attendance list + quiz record
5. **Post-market monitoring:** Q3/2025 report showing KPI deviation < 2 %
6. **Incident ticket:** #INC-2025-09 – “Bias suspicion” – Status: resolved (05 Oct 2025)
7. **Re-Audit:** 12 Oct 2025 – no nonconformities found

All entries are digitally versioned and cryptographically hashed in the **Audit Repository**.

Best Practice Recommendations

- Use a standardized audit trail template with columns: *obligation*, *evidence*, *date*, *responsible*, *status*, *and reference*.
- Enable automated logging through GRC or compliance tools.
- Conduct regular integrity checks (e.g., hash verification).
- Integrate the audit trail into the Conformity Dossier (Art. 17 EU AI Act).

© A4Q Copyright 2025

14.3 Typical Audit Findings and Types of Nonconformities

Type of Nonconformity	Description	Consequence
Formal Nonconformity	Missing or outdated documentation (e.g., no model versioning system)	Requirement for corrective action
Functional Nonconformity	Incomplete implementation of legal obligations (e.g., no human oversight process)	Temporary operational restriction
Severe Nonconformity	Systemic violation of fundamental rights (e.g., bias without mitigation measures)	Administrative fine or operational ban
Procedural Nonconformity	Missing incident-handling process or inadequate audit follow-up	Mandatory corrective measure
Communication Deficiency	Users not properly informed about AI use (Art. 13 / 52)	Warning, reputational damage

14.4 Sanctions under the EU AI Act (Art. 71)

Violation	Maximum Penalty
Use of prohibited AI practices (Art. 5)	up to €30 million or 6 % of global annual turnover
Violation of obligations for high-risk systems (Art. 9–15)	up to €20 million or 4 % of global turnover
Providing false information or failing to notify authorities (Art. 23–24)	up to €10 million or 2 % of global turnover
Non-compliance with enforcement orders	escalating penalties and exclusion from registration

Additionally, authorities may impose sales bans, product recalls, or public warnings.

14.5 Corrective and Improvement Measures

Corrective Actions (CA)

© A4Q Copyright 2025

- Immediate actions to resolve identified nonconformities.
- *Example:* Retraining of the model, adding missing audit trails, and retraining staff.

Preventive / Improvement Actions (PA)

- Structural improvements to prevent recurrence.
- *Example:* Introducing quarterly audit cycles, automated bias checks, or expanding the compliance dashboard.

Audit Follow-up Process

1. Assess the finding → severity and root cause.
2. Develop an action plan with clear deadlines.
3. Approval by the AI Officer and management.
4. Implementation and effectiveness review.
5. Final report and lessons learned.

14.6 Practical Case: Preparing for a High-Risk System Audit

Case Example – Audit of an AI System for Automated Claims Assessment

Context:
An insurance company uses an AI system that automatically reviews submitted claims and recommends payout decisions.
The goal is to reduce processing time and ensure consistent decision-making.
Since the system operates in a sensitive domain, it qualifies as a **high-risk AI system** under Articles 9–24 of the EU AI Act.

Audit Preparation:
In preparation for an internal audit, regulatory evidence is systematically compiled:

- The **AI Officer** prepares an audit checklist based on Articles 9–24 (risk management, data quality, transparency, human oversight, monitoring).
- **Departments** provide all relevant materials: training and test datasets, model documentation, validation reports, log files, and monitoring summaries.
- During a **pre-audit interview** with the auditor, focus areas are defined—particularly bias control (potential discrimination in historical claims data) and fallback mechanisms (human intervention in uncertain cases).

© A4Q Copyright 2025

Audit Execution and Results:
The audit identifies both strengths and areas for improvement:

- **Finding 1:** Annual training for claims managers was outdated.
  → **Corrective Action:** Mandatory retraining within 30 days with documented attendance.
- **Finding 2:** Post-market monitoring lacked an overview of automated decisions by claim type.
  → **Corrective Action:** Introduction of a new dashboard for continuous monitoring of decision trends, error rates, and fairness indicators.

Outcome:
The audit report classifies the system as compliant with minor conditions.
Positive highlights include well-documented processes, structured risk management, and a proactive improvement culture.

After corrective actions:

- Monitoring becomes more data-driven and transparent.
- Human oversight responsibilities are clarified.
- Reporting workflows become more efficient and auditable.

Key Takeaway:
Audits are not merely control mechanisms—they are learning and improvement tools.
Organizations that prepare audits thoroughly, take findings seriously, and document corrective actions increase their compliance maturity, strengthen regulator trust, and lay the foundation for sustainable and accountable AI governance.

14.7 Best Practices for Audit Readiness

Audit readiness is not achieved through isolated measures but through a consistent, organization-wide audit culture.
The following proven practices are particularly effective:

1. **Establish and formalize an Audit Policy**
   Every organization should have a clear, written audit policy defining responsibilities, frequency, and procedures.
   This ensures binding timelines, reporting duties, and full integration into compliance management.
2. **Conduct regular self-audits**
   Semi-annual internal audits promote continuous self-assessment.
   Use an AI Readiness Score to measure progress and identify weaknesses early.

© A4Q Copyright 2025

3. **Maintain version-controlled documentation**
   All audit-relevant materials must be versioned.
   Each change—model, process, or policy—must record what, when, and why it changed.
   This traceability is essential for regulatory and internal reviews.

4. **Leverage cross-audit learning**
   Transfer insights from other audits—such as GDPR data protection, ISO 27001 information security, or ISO/IEC 42001 AI management—into AI compliance.
   This strengthens synergies and fosters consistent quality standards.

5. **Implement training and awareness programs**
   All employees involved in audit processes—auditors, domain experts, developers, managers—should receive regular training.
   The goal is a shared understanding of audit objectives, evidence requirements, and improvement cycles.

6. **Form interdisciplinary audit teams**
   AI audits require expertise from multiple disciplines.
   Recommended composition: Legal, Technical, Ethics, Data Protection, and Compliance.
   Such teams ensure balanced evaluations across technical, legal, and ethical dimensions and enable holistic risk management.

© A4Q Copyright 2025

15 Harmonized Standards & Presumption of Conformity

⏱ **Duration:** 30 minutes

🎯 **Business Outcomes:**

- **BO 15.1:** Participants develop an understanding of the importance of harmonized standards as evidence of compliance.
- **BO 15.2:** Participants are prepared to evaluate current standards and support their practical implementation in projects.

Learning Objectives (LOs)

- **LO 15.1 (K2):** Participants can explain what harmonized European standards are and describe their role within the EU AI Act.
- **LO 15.2 (K2):** Participants can explain the meaning of the “Presumption of Conformity.”
- **LO 15.3 (K3):** Participants can assess which international standards (e.g., ISO/IEC 42001, ISO/IEC 23894) are suitable for implementing compliance requirements.
- **LO 15.4 (K3):** Participants can evaluate the practical benefits of harmonized standards for audit preparation, evidence management, and risk reduction.
- **LO 15.5 (K1):** Participants know the relationship between harmonized standards, technical specifications, and their function as proof instruments within the conformity process.

Key Terms:

Harmonized standard, Presumption of Conformity, CEN, CENELEC, ISO/IEC JTC 1/SC 42, EN standard, DIN, ÖNORM, SNV, standards library, standards mapping, gap analysis, standardization process, CEN/CENELEC JTC 21, cross-audit learning.

Introduction

The EU AI Act defines the fundamental requirements for safe and trustworthy AI systems.
However, the *practical implementation* of these requirements often takes place through harmonized European standards, developed by CEN (European Committee for Standardization) and CENELEC (European Committee for Electrotechnical Standardization).

When such standards are correctly applied, a legal presumption of conformity applies – meaning:

A system that complies with the relevant harmonized standards is presumed to meet the requirements of the EU AI Act, unless proven otherwise.

© A4Q Copyright 2025

Thus, harmonized standards form the essential bridge between legal obligation and technical implementation.

15.1 Definition and Function of Harmonized Standards

Definition:
Harmonized standards are technical specifications published by the European Commission that translate requirements from EU regulations or directives into operational criteria.

Key characteristics:

- They are officially published in the *Official Journal of the European Union* as “harmonized.”
- Their use is voluntary, but they serve as formal evidence of compliance with legal requirements.
- They are regularly updated to reflect new regulatory and technological developments.

Example:
The implementation of ISO/IEC 42001 (AI Management System) and ISO/IEC 23894 (AI Risk Management) can demonstrate that a company systematically fulfills Articles 9–23 of the EU AI Act – thereby establishing a Presumption of Conformity.

15.2 Presumption of Conformity – Legal Background

The Presumption of Conformity is codified in Article 40 of the EU AI Act.
It means that organizations adhering to the technical requirements of harmonized standards are not required to provide separate evidence for compliance with the corresponding legal provisions.

Advantages:

- Reduced verification and documentation effort
- Increased legal certainty in audits and market supervision
- Easier access to CE marking
- Common assessment framework for providers, deployers, and auditors

Important:
Presumption of Conformity does **not** equal automatic exemption.
Organizations must still document:

- Which standards were applied,
- How they were implemented, and
- Any deviations or complementary measures that were adopted.

© A4Q Copyright 2025

15.3 Current Standards Landscape (Selection, 2025)

Standard / Specification	Thematic Area	Relevance for the EU AI Act
ISO/IEC 42001	AI Management System (AIMS)	Structures processes for governance, accountability, and continuous improvement (Art. 17 ff.)
ISO/IEC 23894	AI Risk Management	Operationalizes the risk management obligations under Article 9
ISO/IEC 22989	Concepts and Terminology	Provides a unified vocabulary for documentation and audits
ISO/IEC 23053	Machine Learning Framework	Defines principles for model design, training, and validation
ISO/IEC TR 24028	AI Security and Resilience	Complements Article 15 – Robustness, accuracy, and cybersecurity
DIN SPEC 92001-1 / -2	Quality Requirements for AI	Early national precursor; useful reference for internal AI policies
ISO/IEC 27001 & 27701	Information and Privacy Management	Relevant for Article 10 (Data Quality) and Article 29 (Operation and Governance)
ISO/IEC 42006 (in development)	Human Oversight and Accountability	Expected in 2026 – supports compliance with Article 14 EU AI Act

15.4 Integration of Harmonized Standards within Organizations

An effective compliance system uses harmonized standards as a framework for governance and evidence management.

Recommended steps:

1. **Conduct a mapping:** Link the relevant articles of the EU AI Act to corresponding standards (e.g., *Art. 9 ↔ ISO/IEC 23894*).

© A4Q Copyright 2025

2. **Perform a gap analysis:** Assess which standard requirements are already met.
3. **Implement processes:** Align internal workflows, roles, and documentation structures with the chosen standards.
4. **Prepare for audits:** Use standard-based checklists (e.g., *DIN EN ISO/IEC 42001 Annex A*).
5. **Ensure continuous improvement:** Review and update compliance processes regularly when standards are revised.

Practical Example: ISO/IEC 42001 as Evidence of Presumption of Conformity

A European medical technology company develops an **AI-based diagnostic tool** that analyzes X-ray images and provides physicians with risk assessments.
Since the system directly influences healthcare decisions, it qualifies as a **high-risk AI system** under Annex III, Section 11 of the EU AI Act (*"Medical devices with an AI component"*).

To systematically implement the legal obligations from Articles 9 to 23 of the AI Act, the company adopts an AI Management System (AIMS) in accordance with ISO/IEC 42001.
This standard establishes a comprehensive governance and control framework comparable to ISO 9001 (quality) or ISO 27001 (security), but specifically designed for AI.

Step 1: Implementation of the AI Management System

The company sets up an AI Governance Board defining policies, responsibilities, and escalation paths.

- **Art. 9 – Risk Management:** A standardized process evaluates technical, ethical, and legal risks.
- **Art. 10 – Data Quality:** A data-governance team reviews all training and validation data for representativeness and bias.
- **Art. 11–15 – Documentation, Logging, Transparency, Human Oversight:**
  The standard requires process manuals, audit logs, and verifiable human-control mechanisms.
- **Art. 17 ff. – Conformity Assessment:** Internal audits and management reviews are conducted at least semi-annually.

Step 2: Training in Accordance with Article 4(4) AI Act

All employees involved in development and validation complete modular training integrated into the quality management system:

- **Developers:** Model validation, bias detection, documentation requirements
- **Clinical experts:** Interpretation of AI results, human-oversight rights

© A4Q Copyright 2025

- **Compliance & IT teams:** Evidence creation, audit preparation, logging procedures

Attendance is digitally recorded and renewed annually, ensuring full compliance with the training obligation under Art. 4(4) in an auditable manner.

Step 3: Versioned Documentation and Traceability

All changes to models, datasets, or processes are centrally tracked in a change-log register.
Each entry includes:

- The reason for change (e.g., new dataset, model retraining)
- Date, responsible person, review record
- Impact on risk or conformity assessment
- Formal approval by the AI Officer

This procedure fulfills the documentation requirements of Art. 11 AI Act and aligns with the ISO/IEC 42001 chapters on *Documented Information* and *Continuous Improvement*.

Step 4: Audit and Recognition by Market Supervision

During an external audit by a **notified body**, the company can demonstrate:

- Which processes, roles, and procedures cover the AI Act obligations,
- That all training and testing activities were properly conducted and recorded, and
- That every modification and evaluation is version-controlled and traceable.

Auditors confirm that, through the application of harmonized standards (especially ISO/IEC 42001 + ISO/IEC 23894), the company has established a systematic, documented, and effective AI compliance management system.

Result:
The market surveillance authority recognizes the company as compliant under Article 40 EU AI Act (*Presumption of Conformity*).

Benefits:

- No need for additional technical testing
- Simplified **CE-marking** process
- Significantly shorter audit review times

Beyond compliance, the management system strengthens internal quality and risk awareness: changes, incidents, and new regulatory requirements are handled quickly and systematically – building a sustainable AI compliance culture that goes beyond minimum legal obligations.

© A4Q Copyright 2025

15.5 Collaboration between CEN/CENELEC and ISO in Standardization

European and international standardization organizations work closely to ensure that AI technical standards are globally consistent rather than conflicting.

- **CEN/CENELEC JTC 21** is the central European committee developing harmonized AI standards that may later form the basis for **Presumption of Conformity** under the EU AI Act.
- It collaborates directly with **ISO/IEC JTC 1/SC 42 (Artificial Intelligence)** – the global committee responsible for AI standards such as **ISO/IEC 42001** (AI Management Systems) and **ISO/IEC 23894** (AI Risk Management).
- The shared goal is **worldwide interoperability** – preventing divergent technical requirements across Europe, the US, and Asia that could hinder certification or international trade.
- Each EU member state maintains **national mirror committees** (e.g., DIN in Germany, ÖNORM in Austria, SNV in Switzerland). These enable companies, universities, and research institutes to actively participate in drafting new AI standards and to contribute practical expertise.

This transparent, participatory process ensures that European values and data-protection principles are embedded in global AI standards from the outset.

15.6 Best Practices for Applying Harmonized Standards

The use of harmonized and internationally recognized standards is not a one-time activity – it is an ongoing process.
Organizations that systematically integrate standards into their governance and quality structures gain greater legal certainty, more efficient audits, and clearer evidence paths for regulators.

Proven best practices:

1. **Build a standards library**
   Establish a centralized repository for all relevant standards, guidelines, and technical specifications – with clear ownership for maintenance and updates.
   Include both European (CEN/CENELEC) and international (ISO/IEC) standards.
   → *Benefit:* All departments work from a single, up-to-date source during audits and certifications.
2. **Integrate standards mapping into policies**
   Reference the applicable standards directly within internal AI policies and procedures.
   Every directive related to AI development, operation, or monitoring should cite the corresponding

© A4Q Copyright 2025

clause (e.g., “in accordance with ISO/IEC 23894 § 6.3 – Risk Assessment”).
→ *Result:* Transparent alignment between internal rules and external audit criteria.

3. **Promote training and awareness**
   Regularly inform teams about standard revisions, new publications, and interpretative updates.
   Use short awareness sessions or newsletters to ensure timely integration of new requirements into projects.

4. **Leverage cross-audit learning**
   Many AI standard requirements overlap with ISO 9001 (quality) and ISO 27001 (information security).
   Reuse documentation templates, audit checklists, and lessons learned from these frameworks to avoid duplication and strengthen quality consistency.

5. **Conduct regular gap analyses**
   At least once per year, review:
   - Whether new or updated AI standards have been published,
   - Which ones are now harmonized, and
   - Whether current internal processes still meet all requirements.
     → *Outcome:* Continuous alignment with evolving regulation and full audit readiness.

© A4Q Copyright 2025

16 Global Interfaces & Export Control

⏱ **Duration:** 60 minutes

🎯 **Business Outcomes:**

- **BO 16.1:** Participants are prepared to assess risks arising from data export, dual-use restrictions, and intellectual property (IP) rights.
- **BO 16.2:** Participants are able to support compliance requirements in international supply chains.

Learning Objectives (LOs)

- **LO 16.1 (K2):** Participants can explain the regulatory risks involved in exporting AI systems and data to third countries.
- **LO 16.2 (K2):** Participants can categorize dual-use restrictions and export controls applicable to AI technologies.
- **LO 16.3 (K2):** Participants are familiar with measures for ensuring lawful international supply chains and data transfers.
- **LO 16.4 (K1):** Participants know the main international topics related to export control, IP rights, and dual-use regulations.
- **LO 16.5 (K1):** Participants understand the basic importance of international agreements and multilateral frameworks for the secure and lawful handling of AI technologies.

Key Terms:

Data export, data localization, dual-use goods, export control, intellectual property rights, license verification, WTO rules, supply-chain compliance, sanctions list, third-country transfer, international agreement, trade law, ITAR/EAR, compliance register.

Introduction

AI systems are increasingly developed, trained, and operated on a global scale.
This creates new risks related to export control, data localization, and intellectual property (IP).
Organizations must ensure that AI models, training data, and components are only used in countries that maintain an adequate level of legal and data protection.

© A4Q Copyright 2025

16.1 Data Export and Data Localization

The cross-border transfer of data is often unavoidable for AI systems – particularly when training, validation, or operational data are processed in global cloud environments.
At the same time, international data transfer represents one of the most sensitive areas of AI compliance, since control over the protection of personal information may be lost once data leave the EU.

Legal Framework

The General Data Protection Regulation (GDPR) governs data transfers in Articles 46 ff., defining the conditions for exporting personal data to countries outside the EU or EEA.
Additionally, Article 10(5) of the EU AI Act requires providers and deployers of high-risk AI systems to ensure that all data-processing activities – including storage and training – comply with applicable data-protection regulations.

In practice:
Even if AI development is globally distributed, the legal responsibility for protecting personal data remains with the European organization that provides or operates the system.

Typical Risks

The primary risk arises from transferring data to “insecure third countries” – jurisdictions that lack an EU-recognized adequate level of data protection.
This can result in affected individuals losing effective rights of access, erasure, or objection.

Other major compliance risks include:

- Unauthorized data sharing or reuse by third parties,
- Data mining without consent,
- or state surveillance and access under national security laws.

Example:
A company trains a language model in a non-EU cloud region. The stored user data are no longer subject to the GDPR. Without adequate safeguards, this constitutes a data-protection violation – potentially resulting in fines under Article 83 GDPR.

Measures for Lawful Cross-Border Data Transfers

To manage these risks, organizations should implement the following safeguards:

1. **Use of approved Standard Contractual Clauses (SCCs):**
   Issued by the European Commission, these contractual templates ensure that non-EU recipients guarantee protection levels comparable to the GDPR.
   They are the primary mechanism for lawful data transfers to countries without adequacy decisions.

© A4Q Copyright 2025

2. **Assessment of the recipient country's adequacy:**
   Before any data transfer, verify whether the EU Commission has recognized the destination country as data-protection compliant.
   Example: The EU–US Data Privacy Framework (2023) allows certified U.S. organizations to receive EU personal data under specific safeguards.
3. **Internal approval procedures for cloud or offshore training data:**
   Any external data processing – especially in non-EU cloud or data centers – should go through a formal internal approval process that evaluates:
   - Location and accountability of data processing,
   - Existence of security certifications (e.g., ISO 27001),
   - Encryption and access-control measures,
   - Contractual guarantees for data return and deletion.
4. **Documentation and monitoring:**
   All international data transfers must be fully traceable and documented – including the involved service providers, the transfer purpose, and the protective mechanisms applied.
   Continuous monitoring ensures that legal changes (e.g., withdrawal of an adequacy decision) are promptly reflected in compliance processes.

16.2 Dual-Use Goods and Export Control

The European Union operates under a unified export control framework that also applies to digital technologies and AI systems.
A particularly relevant category is the so-called dual-use sector – covering goods, software, or technologies that can serve both civilian and military or security-related purposes.

Definition and Legal Framework

The term *"dual-use item"* is defined in Regulation (EU) 2021/821, which establishes a Union regime for the control of exports, brokering, technical assistance, transit, and transfer of dual-use items.
This regulation applies directly in all EU Member States and specifies when an export authorization is required for goods or technologies that could potentially be used for military purposes.

The regulation covers not only physical products but increasingly also intangible digital assets, such as:

- Software used to develop or control autonomous systems,
- AI models for pattern recognition or facial recognition,
- Algorithms for cryptography, network security, or surveillance,

© A4Q Copyright 2025

- Simulation or training datasets used in safety-critical applications.

Relevance for AI Systems

With the rise of advanced AI technologies, software, training data, and AI models may fall under the scope of the Dual-Use Regulation.

For instance, an AI system originally designed for civilian purposes (e.g., industrial image analysis) could potentially be repurposed for military targeting, surveillance, or drone guidance.
Therefore, companies must assess whether a given export – meaning any cross-border transfer or provision – requires authorization.

Examples of AI technologies relevant to dual-use export control:

- Systems for facial or object recognition in video data (potential use in surveillance technologies),
- AI models for autonomous navigation of vehicles or drones,
- Speech recognition systems for security or intelligence applications,
- Software for decryption, cybersecurity, or data analytics in sensitive environments.

These technologies are not prohibited per se, but depending on the destination country, end user, and intended use, they may require an export license or prior assessment by the competent national authorities.

Obligations for EU-Based Organizations

Companies that share AI software, source code, or training data with partners outside the EU must verify whether:

- The export item appears in the EU Dual-Use List (Annex I of Regulation 2021/821),
- The recipient or destination country is listed under EU sanctions or embargoes,
- or the end-use is of potential security concern (e.g., military, surveillance, or weapons development).

Importantly, even intangible transfers – such as uploading models to non-EU cloud systems, sharing code via online repositories, or providing remote access to training servers – are legally considered exports under the regulation.

Practical Measures for AI Organizations

1. **Conduct export control checks before sharing AI software or training data**
   Every external transfer or publication should undergo a structured export review, including:

© A4Q Copyright 2025

- Comparison with the Dual-Use List (especially Category 4 – Information Security, Category 6 – Sensors, Category 9 – Aerospace Technology),
- Verification of the recipient and end-use purpose,
- Obtaining an export license from the relevant national authority, if required.

2. **Document licenses and end-use certificates**
   For any export subject to authorization, complete documentation must be maintained, including:
   - License number or official export authorization,
   - End-user certificate,
   - Statement of intended use by the recipient,
   - Delivery and access logs.
     These records should be retained for at least five years and stored within the organization's compliance management system.
3. **Coordinate with national export control authorities**
   Authorization and enforcement are handled by **national competent authorities**, such as:
   - **BAFA (Federal Office for Economic Affairs and Export Control)** in Germany,
   - **Service Public Fédéral Économie** in Belgium,
   - **Direzione Generale per la Politica Commerciale Internazionale** in Italy,
   - or equivalent ministries in Austria, France, and other EU Member States.
     These agencies provide guidance, review export applications, and issue binding rulings on licensing requirements.

Connection to AI Compliance

Export control forms part of a comprehensive AI governance strategy.
It complements the risk management obligations under Article 9 of the EU AI Act and should be integrated into the organization's compliance framework.

Therefore, the AI Compliance Officer should also be informed about dual-use assessments and coordinate export-related decisions in close collaboration with legal, IT security, and data protection teams.

16.3 IP Rights and Licensing

Artificial intelligence (AI) can generate, modify, or derive content from existing data. This directly implicates core questions of intellectual property (IP). Both the use of training data and the downstream reuse of generated outputs create complex legal requirements in copyright, licensing, and liability.

© A4Q Copyright 2025

Relevance for AI compliance

AI systems do not operate in a legal vacuum: any training material, model, or output may be protected by IP. This includes not only text, images, or music, but also code, databases, and models. Organizations in the EU must ensure that development, training, and deployment comply with applicable IP and licensing rules.

Key questions:

1. Who owns the training data?
2. What rights apply to a model's output?
3. Who is liable for copyright infringements or unauthorized use?

Copyright in training data

Training data underpins every AI system. If it contains protected works—texts, photos, audio recordings, or source code—its use requires a legal basis.

Under the **EU Copyright Directive (Directive (EU) 2019/790)**, **text and data mining (TDM)** for research is generally permitted unless rights holders have opted out.

For **commercial purposes** or training **proprietary** models, a **license** or explicit permission is typically required.

Examples:

- Training an image generator on copyrighted artworks without permission may infringe copyright.
- Using journalistic articles or web content without a license or attribution can violate EU and national copyright laws.

Recommendation: Before any training, verify that datasets are free of IP restrictions and that all license terms are observed.

Open-source licenses and model sharing

Many AI models and frameworks are released under open-source licenses (e.g., MIT, Apache 2.0, GPL, Creative Commons). These ease adoption but require careful review.

- **Obligations:** Depending on the license, you may need to disclose source code, credit authors, or mark modifications.
- **Restrictions:** Some licenses prohibit **commercial use** ("NC" clauses) or **certain domains** (e.g., military).
- **Risk of unclear license chains:** Stacked models/components can create complex, sometimes conflicting obligations.

Example:

A company embeds an open-source speech-to-text model licensed under GPLv3. GPLv3 would require the company's own code to be disclosed if distributed together—creating an unintended disclosure obligation and a compliance risk.

© A4Q Copyright 2025

Recommendation: Conduct a license-compatibility review for any open-source software or AI model before integration—ideally via Legal or an internal Open-Source Compliance team.

Usage rights in AI-generated outputs

Whether AI-generated content is protected by copyright is not yet uniformly settled in the EU. The prevailing view is that copyright requires **human authorship**; purely automated AI output is therefore **not** itself protected.

Practical implications:

- Companies may freely use AI-generated content but should label it as AI-generated (Art. 52 EU AI Act).
- If a human makes a substantial creative contribution (e.g., through targeted prompting, editing, or curating), derivative human authorship may arise.
- Conflicts occur where outputs derive from protected training material (e.g., a generated image imitating a distinctive living artist's style).

Recommendation: Maintain an internal record for all generated content, including:

- the models and prompts used,
- sources and licenses of training material,
- the intended use (internal, commercial, public).

Contracts and liability

Legally sound AI use requires clear contracts among all parties—providers, developers, licensors, and customers.

Core elements:

- **License due diligence prior to training and deployment:** Verify lawful use of training data, libraries, and model components.
- **Source and rights documentation:** Maintain a **license register** covering versions, sources, terms, and accountable owners.
- **Liability and pass-through clauses:** Contracts with AI vendors should set out IP ownership, liability caps, indemnities, and use restrictions. For generative systems, clarify who bears liability for **potential IP infringement in outputs** and how third-party claims are handled.

Example:

A publisher uses a generative text model to summarize scholarly articles. An author alleges that a summary reproduces protected expression. With no contractual allocation of risk for AI outputs, the publisher bears full liability.

© A4Q Copyright 2025

Conclusion

IP and licensing are central to AI compliance—especially when systems are trained on third-party data or outputs are used commercially. EU organizations should ensure that:

- training data and models are lawfully acquired or licensed,
- all licenses and copyrights are documented,
- contracts define ownership, liability, and onward use.

A systematic IP-compliance program protects not only against legal exposure but also reputational and market risks. Over time, it strengthens transparency, traceability, and trust—key goals of the EU AI Act and the EU's broader digital strategy.

16.4 Compliance in International Supply Chains

AI today is built in globally networked supply chains: training data from multiple regions, models hosted in international clouds, and components (software modules, sensors) sourced from non-EU vendors. Compliance therefore spans the entire value chain. EU companies are responsible not only for their own systems, but also for the legal and ethical conformity of third-party AI components.

EU-wide compliance significance

The EU AI Act has extraterritorial reach: it applies to providers and deployers outside the EU if their AI systems are placed on the EU market or used in the EU. Consequently, EU companies must ensure that international partners adhere to the Act's principles, regardless of where those partners are located.

Common challenges:

- Divergent third-country legal regimes,
- Lack of harmonization in privacy, product liability, and safety,
- Sanctions and embargoes restricting certain technology or data exports,
- Limited transparency on provenance, training data, or model versions of supplied AI components.

Risks in global AI supply chains

1. **Regulatory risk:** Non-EU suppliers may deliver components that don't meet EU AI Act or GDPR requirements. If integrated and marketed in the EU, the EU provider can be liable.
2. **Sanctions/export risk:** Transfers of models or datasets to restricted destinations can breach EU sanctions or dual-use rules.
3. **Cyber/data security risk:** Third parties may gain access to sensitive data via cloud/API, threatening privacy and security.

© A4Q Copyright 2025

4. **Reputational risk:** Human-rights issues, unethical data practices, or discriminatory algorithms at suppliers can damage the EU prime contractor's reputation.

Example:
A European carmaker sources a driver-monitoring face recognition module from a non-EU vendor. Later testing reveals bias due to skewed training data. Despite indirect responsibility, the OEM is criticized for insufficient supplier oversight.

Recommended measures for compliant supply chains

1. **Supplier audits for AI compliance and privacy**
    - Audit suppliers that provide models, training data, or automated decision logic.
    - Check documentation, explainability, and alignment with EU AI Act principles (risk management, transparency, human oversight).
    - Require GDPR compliance evidence: data sources, deletion schemes, security controls.
    - Obtain reports on bias, fairness, and ethical standards.
2. **Contractual commitment to EU-AI-Act principles**
    - Bind suppliers to key duties (Arts. 9–15: risk management, data quality, transparency, human oversight, robustness).
    - Require technical documentation and audit data; immediate notice of model or dataset changes.
    - Add ethics/transparency clauses: no unlawfully collected data, clear labeling of AI-generated content, documentation of training sources.
    - For high-risk systems, include shared liability terms and audit rights.
3. **Global compliance register with evidence**
    - Maintain a central register of all AI systems, modules, and supplier relationships, including:
        - supplier identity and location,
        - type of AI system/module,
        - risk level under the EU AI Act,
        - last compliance assessment,
        - accountable persons and approval date.
    - Keep it updated to support internal/external audits.
      Tip: Integrate with supplier-management or GRC platforms and with ISO 9001 / ISO 42001 documentation.

Links to other EU regulations

© A4Q Copyright 2025

- **CSDDD** (Corporate Sustainability Due Diligence Directive): due diligence on human rights and environment in supply chains.
- **DSA** and **Data Act**: govern data sharing/usage across borders.
- **GDPR** and **EU AI Act**: define technical/organizational duties for international data exchange and AI operations.

Conclusion

Global supply chains are the backbone of modern AI—and a critical compliance arena. By documenting suppliers, data flows, and model dependencies, organizations establish the basis for lawful and ethical AI. Those that implement:

- regular supplier audits,
- contractual EU-standard obligations, and
- a central compliance register,
  can materially reduce regulatory risk and credibly demonstrate the Presumption of Conformity (Art. 40 EU AI Act) to authorities. The result is an end-to-end AI compliance chain—from development and cross-border data transfer to responsible use in the EU single market.

© A4Q Copyright 2025

17 Optional – Practical Exercises & Case Studies

🎯 **Business Outcomes:**

- **BO 17.1:** Participants develop practical competence in applying key AI compliance concepts such as risk classification, FRIA, and GPAI obligations.
- **BO 17.2:** Participants are able to develop compliance artifacts, including documentation, labeling concepts, and monitoring plans.

Introduction

This optional exercise module provides flexibility for trainers to deepen specific syllabus topics and tailor content to the participants' needs and prior knowledge.
The **selection, scope, and depth** of exercises lie at the **discretion of the training provider** and should reflect the thematic focus of the respective course (e.g., technical, legal, or organizational aspects of AI compliance).

The goal is to **reinforce understanding** of roles, responsibilities, and evidence requirements through interactive and practical learning methods, while supporting the **transfer to real-world organizational contexts**.

Examples of optional exercise formats:

In-depth case studies on selected EU AI Act articles (e.g., Arts. 9–15, 27, 52)

- Simulation of an internal or external audit ("AI Compliance Assessment")
- Creation of a sample compliance dossier or monitoring plan
- Role-play: communication between oversight, management, and development teams
- Comparative exercise: implementation of national AI regulations outside the EU (e.g., UK, Canada, China)
- Analysis of real-world examples from various sectors (e.g., healthcare, finance, public administration)

These exercises are not part of the certification exam, but they can significantly enhance practical confidence and audit-readiness, especially in extended training programs or in-house workshops.

17.1 Introduction to AI Compliance & the EU AI Act

These introductory exercises reinforce the basic concepts and terminology of the EU AI Act. Participants learn to correctly understand and apply definitions, roles, and transition timelines.

© A4Q Copyright 2025

Exercises:

• Matching activity: correctly assign the terms *AI System*, *GPAI*, *Provider*, and *Deployer*

• Discussion: the impact of the EU AI Act on your own organization

• Timeline exercise: arrange the transition periods 2024–2027 in the correct order

• Reflection: benefits and risks of AI from a compliance perspective

17.2 Risk-Based Approach and Classification

This session deepens understanding of the four AI risk levels and trains participants to classify real-world AI applications appropriately.

Exercises:

• Case classification: assign examples as high-, limited-, or minimal-risk

• Mapping: match AI use cases to the categories in Annex III

• Develop a decision tree: determine the risk level based on typical parameters

• Group reflection: evaluate transitions between risk levels

17.3 Global and Sector-Specific Regulatory Landscape

The purpose of this session is to understand the global perspective of AI regulation and identify commonalities and differences among major frameworks.

Exercises:

• Comparison activity: align regulatory approaches of the EU, USA, China, UK, and OECD

• Mapping: identify overlaps between the EU AI Act and ISO/IEC 42001

• Discussion: implications of divergent legal systems for multinational enterprises

• Group task: identify risks in international AI projects

17.4 Prohibited AI Practices (Art. 5)

This unit focuses on the ethical and legal evaluation of prohibited AI practices. Participants learn to identify problematic applications and interpret the exceptions defined under Article 5.

Exercises:

• Case analysis: identify prohibited AI practices

• Matching activity: assign exceptions (e.g., law enforcement) to the corresponding legal conditions

• Group work: define risk factors for unintentional violations

• Discussion: ethical limits versus technological possibilities

© A4Q Copyright 2025

17.5 High-Risk AI Systems and Obligations (Arts. 6–51)

This session trains participants to apply the obligations and responsibilities related to high-risk systems in practice.

Exercises:

- Matching task: assign article numbers to the respective compliance requirements
- Checklist exercise: identify what documentation and evidence are required for high-risk systems
- Role analysis: distinguish between provider and deployer responsibilities
- Short case: identify a high-risk system and derive the applicable obligations

17.6 Risk Management & Quality Management Systems

In this unit, participants practically apply the concepts from ISO/IEC 23894 and ISO/IEC 42001, linking risk analysis with AI management system processes.

Exercises:

- Process exercise: design a risk assessment according to ISO/IEC 23894
- Governance mapping: integrate AI risk management into existing management systems
- Group activity: create a risk matrix for an AI project
- Comparison: difference between FRIA and AI risk management

17.7 Conformity Assessment and CE Marking

This exercise focuses on understanding how conformity assessment processes work in practice and which documents are required.

Exercises:

- Practical checklist: steps for internal conformity assessment
- Matching activity: technical documentation ↔ article requirements
- Group exercise: create a mini CE-declaration for an example system
- Discussion: advantages and disadvantages of internal versus external assessments

17.8 Transparency Obligations for Limited-Risk Systems (Art. 52)

Participants design transparency notices and evaluate their effectiveness to better understand labeling obligations.

Exercises:

- Practical exercise: design a transparency label (text, metadata, UI notice)
- Review activity: plan an A/B test for chatbot labeling

© A4Q Copyright 2025

• Mini-case: identify transparency violations
• Discussion: how openness influences user trust

17.9 General-Purpose AI (GPAI) & Systemic Risk

This session covers Articles 53–55 of the EU AI Act and trains participants to implement GPAI-related obligations within their organization.

Exercises:

• Exercise: allocate GPAI obligations (Arts. 53–55) between providers and users
• Analysis: evaluate a transparency report of a GPAI provider
• Group work: create a checklist for GPAI integration in the company
• Brainstorming: plan Red-Team-Testing as a voluntary best practice

17.10 Fundamental Rights Impact Assessment (FRIA, Art. 27)

These exercises allow participants to experience the FRIA methodology in practice and understand the relationship between fundamental rights and AI applications.

Exercises:

• Mini-FRIA: identify affected fundamental rights and associated risks
• Evaluation exercise: build a severity matrix for potential rights violations
• Case comparison: distinguish between FRIA and DPIA (Data Protection Impact Assessment)
• Discussion: how FRIA is integrated into governance and decision-making processes

17.11 Post-Market Monitoring, Reporting & Market Surveillance

This unit focuses on monitoring obligations after placing AI systems on the market and on incident-reporting duties under Articles 23 ff. of the EU AI Act.

Exercises:

• Design exercise: create a monitoring plan with key performance and risk indicators.
• Checklist: develop an incident-reporting process according to Article 23.
• Group simulation: model the workflow of a serious-incident case.
• Reflection: what documentation must be retained for long-term compliance evidence?

17.12 Governance, Organization & Roles

This section emphasizes cooperation, coordination, and defined responsibilities within AI-compliance structures.

© A4Q Copyright 2025

Exercises:

• Role-play: collaboration between AI Officer, Data Protection, and IT teams.

• Create a RACI (responsible–accountable–consulted–informed) matrix.

• Group task: design the structure of an internal AI Compliance Committee.

• Exercise: develop a training plan according to Article 4(4).

17.13 Minimal-Risk Systems & Voluntary Governance ("Ethical AI")

This unit demonstrates how ethical frameworks can be applied voluntarily, even when not legally mandated.

Exercises:

• Guideline comparison: ISO/IEC 42001 / OECD / UNESCO AI Ethics principles.

• Workshop: apply a short-form Ethical Impact Assessment (EIA).

• Group task: link CSR or ESG objectives to AI projects.

• Reflection: defining ethical minimum standards beyond legal obligations.

17.14 Audit Readiness, Audit Trails & Sanctions

These exercises train participants in audit preparation, documentation review, and handling of common audit findings.

Exercises:

• Simulation: internal audit interview (auditor ↔ AI officer).

• Checklist review: documentation status versus compliance requirements.

• Matching exercise: link typical findings to corrective actions.

• Practical task: draft an audit policy template.

17.15 Harmonized Standards & Presumption of Conformity

This unit focuses on how harmonized standards interact with the EU AI Act and support conformity evidence.

Exercises:

• Mapping exercise: ISO/IEC 42001 requirements ↔ relevant AI Act articles.

• Group work: design the structure of an internal standards library.

• Exercise: perform a gap analysis for current standard revisions.

• Comparison: DIN vs. CEN/CENELEC – differences in application and scope.

© A4Q Copyright 2025

17.16 Global Interfaces & Export Control

This session examines international supply chains and export-control obligations for AI systems.

Exercises:

- Checklist: combine export-control and AI-compliance requirements.
- Exercise: conduct a risk analysis for third-country supply chains.
- Group work: develop a supplier-audit plan based on AI Act criteria.
- Discussion: achieving harmonization despite differing legal frameworks.

17.17 Optional Exercise Module – Advanced or Supplementary Practice Tasks

This optional section offers additional, advanced exercises that can be selected depending on the course scope and participant experience.
Trainers may use these activities to reinforce specific competencies or to deepen the understanding of cross-cutting compliance topics.

17.18 Optional Chapter – Roadmap & Readiness Assessment 2025 – 2027

This session supports organizations in planning their strategic AI Act readiness phases and setting measurable implementation priorities.

Exercises:

- Exercise: perform a gap analysis of the organization's current AI compliance status.
- Prioritization task: identify "quick wins" and long-term actions.
- Checklist: evaluate overall compliance maturity.
- Group work: draft a three-year AI compliance roadmap (2025 – 2027).

17.19 Optional Chapter – Future Trends & Evolution of the Regulatory Framework

This final unit provides a forward-looking perspective on emerging AI governance roles and international convergence of standards.

Exercises:

- Trend analysis: outline new roles (AI Auditor, AI Board, AI Safety Officer).
- Discussion: assess potential risks associated with Frontier AI models.
- Reflection: analyze international convergence between the EU, USA and Asia.
- Group exercise: design a "Future Compliance 2030" audit scenario.

© A4Q Copyright 2025

18 Roadmap & Readiness Assessment 2025–2027

Note: This chapter is not exam-relevant and serves as optional enrichment for training providers.

🎯 **Business Outcomes**

- **BO 18.1:** Participants are prepared to create an AI compliance roadmap with implementation priorities.
- **BO 18.2:** Participants are equipped to assess the organization's maturity with respect to AI Act readiness.

Non-exam Learning Objectives (LOs)

- **LO 18.1 (K2):** Explain how organizations can assess their EU AI Act implementation status using a maturity model.
- **LO 18.2 (K2):** Understand the purpose of an AI compliance roadmap and describe key steps in phased implementation (gap analysis, prioritization, action planning).
- **LO 18.3 (K3):** Conduct and interpret a simple self-assessment based on an ISO/IEC 42001–aligned maturity model.
- **LO 18.4 (K2):** Name key tools (checklists, FRIA template, conformity dossier, governance policy) and explain their purpose in the compliance process.
- **LO 18.5 (K3):** Design an AI-Act-readiness roadmap for a practical case, including responsibilities, training measures, and documentation processes.
- **LO 18.6 (K1):** Know the link between continuous improvement, audit trail, and reporting in AI compliance.

Key terms:
AI readiness, maturity model, maturity level, self-assessment, gap analysis, compliance roadmap, AI compliance checklist, FRIA template, conformity dossier, governance policy, training matrix, responsibility assignment, role model, ISO/IEC 42001 alignment, documentation standard, reporting structure, progress measurement, continuous improvement, audit trail, AI register.

Introduction / Purpose

This optional chapter offers a practical guide for organizations to implement the EU AI Act systematically and efficiently. It links regulatory requirements with management methods and shows how to develop quick wins, priorities, and long-term governance structures along an AI compliance roadmap.

© A4Q Copyright 2025

18.1 Building Blocks of an AI Compliance Roadmap

A robust roadmap should cover strategic, organizational, and technical workstreams. It specifies **what** to do, **when**, and **by whom**.

Phase	Timeframe (guidance)	Focus	Example Activities
1 – Initialization	2025 Q1–Q2	Awareness & inventory	Executive training · Inventory of all AI systems · Initial gap analysis
2 – Risk assessment & classification	2025 Q2–Q3	Classification under Arts. 6–9 AI Act	Map all systems to risk levels · FRIA check for public bodies
3 – Regulatory integration	2025 Q3–Q4	Process & policy setup	Draft AI policy, role descriptions, governance board
4 – Operationalization	2026–2027	Implementation & oversight	Conformity assessment, monitoring plan, audits, reporting
5 – Optimization & maturity uplift	from 2027	Continuous improvement	Combine with ISO/IEC 42001, lessons learned, benchmarking

Note: Training providers decide which phases, exercises, or templates to deepen based on audience and focus.

18.2 Typical Quick Wins and Priorities

The step-by-step implementation of the EU AI Act requirements requires clear priorities. The following measures have proven particularly effective in practice and can serve as a starting point for an AI compliance roadmap in almost any organization.

1) AI system inventory

Create a central inventory of all deployed or planned AI systems, capturing at minimum:

- Purpose and scope,
- Responsible person or unit,

© A4Q Copyright 2025

- Assigned risk class per Arts. 6–9 EU AI Act,
- Current status (pilot, production, decommissioned),
- Evidence of conformity and monitoring.

This register provides transparency and a starting point for risk assessment, auditing, and regulator communication.

2) Staff training

Awareness among specialists and leadership is critical. Training should explain:

- Obligations arising from the EU AI Act,
- Roles and responsibilities (e.g., AI Officer, business owner),
- How to identify and handle risks, incidents, and documentation duties in day-to-day work.

Use tiered programs: a baseline for everyone plus deep dives for key roles.

3) Governance documents

Anchor AI compliance through binding governance artifacts, including:

- An **AI policy** guiding development, deployment, and oversight,
- **Role & responsibility** descriptions (AI Officer, compliance leads, system owners),
- **Escalation & reporting** processes for incidents, risks, or changes.

These strengthen internal controls and integrate AI compliance with existing management systems.

4) Pilot audits

Run pilot audits to test documentation and implementation in practice. Check whether:

- Required evidence under Arts. 9–24 is complete,
- Transparency and logging processes work,
- Communication between business, compliance, and engineering flows smoothly.

Findings inform improvements to processes, training, and documentation quality.

5) Gap analysis

Compare current practice with EU AI Act requirements (notably Arts. 5–24) to identify actions. Typical fields:

- Presence of a risk-management system,
- Completeness of technical documentation,
- Fulfillment of transparency and human oversight duties,
- Training and governance structures.

The result drives a prioritized implementation plan within the AI compliance roadmap.

© A4Q Copyright 2025

18.3 Self-Assessment of AI Compliance Maturity

Organizations are at different stages in their journey toward full implementation of the EU AI Act.
A structured maturity model allows a realistic self-assessment of the current status and supports the prioritization of further actions.
The following model outlines five levels of organizational maturity in managing AI compliance. It can serve as a reference framework for internal assessments, audits, or strategic discussions.

Level	Title	Description	Typical Indicators
1 – Ad hoc	Initial, uncoordinated AI activities	AI systems are deployed without structured evaluation. There is no centralized documentation or responsibility assignment.	No AI policy, undefined roles, no training records.
2 – Emerging awareness	Building regulatory understanding	The organization recognizes the importance of the EU AI Act and begins identifying AI use cases and assigning responsibilities.	Initial system inventory, basic management training, and first compliance checklists.
3 – Structured	Establishment of basic compliance processes	Risk assessments and documentation follow standardized procedures. Initial templates and internal policies are implemented.	AI system register available, FRIA template adopted, responsibilities formally defined.
4 – Integrated	Embedded in the management system	AI compliance is part of corporate governance and integrated into existing management systems. Auditing and monitoring processes are established.	Integration with ISO/IEC 42001 or ISO 9001, regular internal audits, active monitoring plan.
5 – Optimized	Strategic and continuously improving compliance	AI compliance is strategically anchored, managed by KPIs, and externally verified. The organization uses benchmarking for ongoing improvement.	KPI-based reporting, benchmarking with best practices, external certification, or trust label.

Practical Exercise (Suggestion)

Conduct a readiness self-assessment for your organization.

© A4Q Copyright 2025

Using the five levels, determine your current maturity stage and identify the actions required to progress to the next level.

Typical discussion questions:

- Which elements of an AI compliance structure are already in place?
- Where are the remaining gaps compared to the EU AI Act requirements (Arts. 5–55)?
- Which processes should be implemented or improved in the short term?

The results can serve as a foundation for developing an organization-specific AI compliance roadmap.

18.4 Tools and Resources for Roadmap Development

To support the practical implementation of an AI compliance roadmap, organizations can use various standardized tools and templates.
These instruments enable structured planning, documentation, and evaluation of **AI Act readiness** and can be adapted to the size, industry, and complexity of the organization.

AI Compliance Checklist (Arts. 5–55 EU AI Act)
A comprehensive checklist covering all core requirements of the EU AI Act – from prohibited practices (Art. 5) and high-risk obligations (Arts. 9–24) to transparency and GPAI provisions (Arts. 52–55).
It allows systematic self-assessment and serves as a foundation for internal audits or gap analyses.

FRIA Template (Art. 27 EU AI Act)
The *Fundamental Rights Impact Assessment* (FRIA) template supports, in particular, public authorities and operators of high-risk AI systems in evaluating potential fundamental rights risks.
It includes structured guiding questions about affected rights, possible impacts, mitigation measures, and evidence of stakeholder involvement.
The FRIA can complement the *Data Protection Impact Assessment* (DPIA).

Conformity Dossier Template (Arts. 11–23 EU AI Act)
This template forms the basis for the technical documentation and evidence collection required in the conformity assessment process.
It typically includes sections on:

- System description and purpose,
- Training and testing data,
- Risk management and quality assurance,
- Human oversight and monitoring processes,

© A4Q Copyright 2025

- Audit trails, logging, and fallback mechanisms.
  The dossier serves as documentation for supervisory authorities and internal audit bodies.

Governance Policy Template (Arts. 4(4), 29 EU AI Act)
This policy template defines key organizational rules for handling AI within the company.
It outlines:

- Roles and responsibilities (e.g., AI Officer, compliance manager, business owner),
- Escalation and communication channels,
- Principles for training, documentation, and incident management.
  The AI Governance Policy ensures accountability and clarity about internal processes and responsibilities.

Training Matrix by Roles and Responsibilities
A structured overview specifying which employee groups require which training content.
Examples:

- **Developers:** Model validation, documentation duties, bias control
- **Product managers:** Application limits, CE conformity, governance processes
- **Executives:** Liability, strategic accountability, audit preparation
  The matrix provides evidence under Art. 4(4) AI Act that all relevant employees are properly trained and qualified.

Maturity Self-Assessment Questionnaire (based on ISO/IEC 42001)
A practical tool for assessing an organization's current level of AI governance and compliance maturity.
Aligned with the principles of ISO/IEC 42001 (*AI Management System*), it covers topics such as role allocation, risk management, monitoring, transparency, and continuous improvement.
It can be used annually to document measurable progress and prioritize improvement actions.

Note:
Using standardized checklists, templates, and assessment tools facilitates the systematic implementation of AI compliance requirements and promotes consistent, auditable documentation.

Training providers can incorporate these tools into workshops or group exercises to prepare participants for developing their own AI compliance roadmap.

18.5 Conclusion

The AI compliance roadmap links legal obligations with practical implementation management.
Organizations that assess their readiness early, set clear priorities, and establish binding actions not only

© A4Q Copyright 2025

reduce non-compliance and sanction risks but also gain strategic confidence and stakeholder trust – advancing toward sustainable and responsible AI governance.

© A4Q Copyright 2025

19 Future Outlook & Evolution of the Regulatory Framework

Note: This chapter is not part of the examination content and serves as an optional extension for training providers.

🎯 **Business Outcomes**

- **BO 19.1:** Participants develop awareness of upcoming trends (Frontier AI, AI Safety Institute, etc.).
- **BO 19.2:** Participants are prepared to plan and communicate strategic adjustments for future regulatory cycles.

Non-exam Learning Objectives (LOs)

- **LO 19.1 (K1):** Participants know the main future developments of the EU AI Act (guidelines, delegated acts, AI Act 2.0).
- **LO 19.2 (K2):** Participants can explain how complementary legislative acts (Data Act, CRA, DSA, AI Liability Directive) interconnect and expand the AI compliance landscape.
- **LO 19.3 (K2):** Participants can describe the role of the AI Office and the AI Board within the European governance framework.
- **LO 19.4 (K3):** Participants can evaluate international developments (USA, UK, China, G7, OECD, UN) regarding convergence, divergence, and implications for EU organizations.
- **LO 19.5 (K2):** Participants can explain the future importance of voluntary standards and certifications (e.g., AI Trust Label, re-certification, Frontier Model Regulation) for compliance practice.
- **LO 19.6 (K3):** Participants can reflect on which competencies and governance mechanisms organizations will need to proactively adapt to future regulatory changes.

Key Terms:
Delegated Act, Guidelines, AI Act 2.0, Frontier AI Regulation, AI Trust Label, Certification, Annual Re-certification, AI Liability Directive, Data Act, Cyber Resilience Act (CRA), Digital Services Act (DSA), AI Office, AI Board, Global Harmonization, International Cooperation, U.S. AI Executive Order, U.K. AI Safety Summit, China Generative AI Regulation, G7 Code of Conduct, UN AI Governance Initiative, OECD Framework, Transparency Requirements, Model Evaluation, Regulatory Convergence, Future Trends.

Purpose and Context

This optional chapter provides a forward-looking perspective on the future of European and international AI regulation. It aims to help organizations anticipate developments, respond strategically, and adapt

© A4Q Copyright 2025

compliance structures to upcoming requirements.
As the technological landscape evolves rapidly – with *Frontier Models*, autonomous agents, and multimodal systems – compliance professionals must stay informed about emerging political, technical, and ethical trends.

19.1 European Institutions and Governance Structures (Timeline 2025–2030)

The implementation and evolution of the EU AI Act are supported by several newly established or expanded European institutions designed to ensure coordinated, consistent, and forward-looking supervision of artificial intelligence.
These structures are currently being set up (as of 2025) and are expected to become fully operational by 2027.

AI Office (European Commission)

The AI Office serves as the central EU coordination and supervisory body for the enforcement of the AI Act.
Its core tasks include:

- Overseeing the consistent application of the EU AI Act,
- Recognizing harmonized standards and technical specifications,
- Managing the European database for *General Purpose AI (GPAI)* as defined in Articles 53–55,
- Supporting Member States in market surveillance, audits, and guideline development.

From 2026 onward, the AI Office is also expected to take on responsibilities for systemic risk monitoring of large-scale AI models.

European AI Board

The European AI Board is a network of national supervisory and market surveillance authorities across EU Member States.
Its objectives include:

- Exchanging experiences from national implementation,
- Developing common interpretation guidelines for the AI Act,
- Promoting a harmonized application across the Union.

The Board works closely with the European Commission, the European Data Protection Board (EDPB), and standardization bodies such as CEN/CENELEC.
Operational activities are expected to begin by the end of 2025.

© A4Q Copyright 2025

AI Safety Institute (planned)

To strengthen the technological safety of *Frontier AI* systems, a European AI Safety Institute is planned for establishment by 2027.
Its goals include:

- Conducting robustness and safety analyses of large-scale models,
- Evaluating potential systemic risks and misuse scenarios,
- Developing shared testing and evaluation standards for advanced AI systems.

The institute will collaborate with national research centers, security agencies, and European standardization bodies (CEN/CENELEC, ISO/IEC).

International Cooperation

The EU is pursuing a global alignment of AI governance frameworks. Between 2025 and 2030, international partnerships and policy dialogues will intensify, notably with:

- **OECD** (Principles on AI),
- **UNESCO** (Ethical AI Framework),
- **G7** (*Hiroshima Process* – Frontier AI Safety Commitments), and
- **Council of Europe**, which is preparing a convention on AI, human rights, and democracy.

This cooperation aims to ensure that European standards for safety, ethics, and governance gain international recognition – fostering convergent global regulation for AI systems.

19.2 Frontier AI and Systemic Risk (Time Horizon 2025–2030)

The term “Frontier AI” refers to highly capable AI models that, due to their scale, generalization ability, and autonomy, have the potential to create *systemic effects* on the economy, security, information ecosystems, and social structures.
This includes models from the GPT-5 generation and beyond, multimodal language–vision models, autonomous agent networks, and simulation or decision engines deployed in critical infrastructure.

As these systems become more powerful, they introduce new challenges for governance, safety, and oversight.
European and international institutions are therefore working (2025–2030) on a multi-layered regulatory and testing framework to assess and manage the risks of large-scale AI models.

Key developments:

- **Evaluation of systemic risks of large models:**
  Future assessments will move beyond single-function evaluation toward measuring a model’s

© A4Q Copyright 2025

overall impact on society.
Main topics include *disinformation*, *algorithmic amplification of social divisions*, *impacts on critical infrastructures*, and *potential misuse for cybersecurity or defense purposes*.

- **Establishment of international AI safety benchmarks:**
  By 2027, shared evaluation procedures ("benchmarks") for frontier models are expected to be established.
  These will include standardized *transparency reports*, *red-team testing* (targeted safety and misuse testing), *robustness metrics*, and *explainability evaluations*.

- **Debate on licensing and reporting obligations:**
  Between 2026 and 2028, the EU is expected to explore licensing requirements for highly capable models.
  The goal is to obligate large-model providers to document security-relevant properties, report incidents, and demonstrate safeguards before models are released to the public.

- **Establishment of a European AI Safety Lab:**
  By 2028, a central European testing and research center ("AI Safety Lab") is planned to conduct safety, fairness, and robustness testing for frontier models.
  The lab will likely operate under the AI Office, in close cooperation with the planned AI Safety Institute, national research centers, and standardization bodies (CEN/CENELEC JTC 21, ISO/IEC SC 42).

Objective:
This multi-step regulatory approach aims to ensure that high-performance AI models become more *transparent, secure, and controllable* – without hindering innovation or competitiveness in the EU.
Frontier AI is thus seen as a key domain for future governance and safety strategy in Europe.

19.3 Expected Evolution of the AI Act (2025–2030)

With the EU AI Act entering into force in 2024, a continuous regulatory development process begins. Between 2025 and 2030, several delegated acts, guidelines, and complementary legal instruments will further specify and expand the Act to align with technological progress.

Guidelines and Delegated Acts
Starting in 2026, the European Commission plans a series of delegated acts and implementing regulations to operationalize detailed requirements, including:

- Bias metrics and fairness indicators, including sector-specific evaluation standards,
- Logging and audit standards for high-risk systems,
- Methodological guidelines for the FRIA (Fundamental Rights Impact Assessment) under Article 27,

© A4Q Copyright 2025

- Extended documentation duties for General Purpose AI (GPAI).

These clarifications aim to create *uniform European benchmarks* and improve the comparability of regulatory assessments.

Second Regulatory Wave ("AI Act 2.0")
Between 2027 and 2030, a second regulatory wave, often referred to as "AI Act 2.0," is anticipated.
Its likely focus areas include:

- Oversight of Frontier Models and GPAI systems,
- Introduction of a European safety certification for AI systems,
- Establishment of a coherent GPAI ecosystem with tiered responsibilities for developers, providers, and deployers.

Integration with Other EU Frameworks
The AI Act is evolving into an integral part of the broader European digital regulatory framework, closely interconnected with:

- The **Data Act** (data access and usage obligations),
- The **Cyber Resilience Act (CRA)** (security for connected products),
- The **Digital Services Act (DSA)** (content and platform responsibility),
- And the upcoming **AI Liability Directive** (liability for damages caused by AI systems).

This regulatory interlinkage requires companies to align compliance, risk, and IT management systems to avoid duplication and inconsistencies.

Enhanced Governance and Auditing Obligations
From 2028 onward, annual recertifications may be introduced for specific high-risk or frontier AI systems.
Additionally, a "EU AI Trust Label" is under discussion to recognize organizations with demonstrably high standards of compliance and governance – strengthening transparency and public trust in European AI products.

19.4 Global Trends and International Convergence (2025–2030)

AI regulation is increasingly becoming a global issue.
Between 2025 and 2030, several international developments indicate a trend toward stronger regulatory convergence and mutual recognition of AI compliance certifications.

United States – AI Executive Order (2023)
The U.S. "Executive Order on Safe, Secure, and Trustworthy AI" introduced binding safety, bias, and cybersecurity evaluations for government-funded AI systems.

© A4Q Copyright 2025

Agencies such as NIST and DARPA are developing reference frameworks that are also influencing European standardization efforts.

United Kingdom – AI Safety Summit and Frontier AI Taskforce

Through the AI Safety Summit (initiated in 2023, ongoing through 2030) and the Frontier AI Taskforce, the UK promotes a risk-based approach focusing on model testing, safety benchmarks, and "responsibility by design."

Close cooperation with the EU is foreseen, especially regarding safety certifications and audit methodologies.

China – Regulation of Generative AI Services

Since 2024, China has enacted comprehensive rules for "Generative AI Services," including mandatory data labeling, state safety assessments before model deployment, and content alignment with public value standards.

These measures illustrate the growing *geopolitical significance* of AI governance.

OECD and UNESCO – Global Ethical Frameworks

The OECD AI Principles and UNESCO's Ethical AI Framework form the global reference foundation for *fairness, transparency, and accountability*.

The EU aligns with these frameworks to ensure international compatibility and reciprocal recognition of AI governance standards.

Conclusion:

By 2030, a gradual convergence of European, U.S., and Asian AI regulations is expected.

Organizations operating internationally will benefit from harmonized standards – but must also navigate parallel reporting duties and divergent evidentiary requirements across jurisdictions.

19.5 Strategic Implications for Organizations (Time Horizon 2025–2030)

The upcoming regulatory cycles will require European organizations to demonstrate a high degree of strategic adaptability.

AI compliance will evolve from a purely legal obligation into a continuous management process, integrating governance, technology, ethics, and risk management.

Proactive Compliance Strategy

Organizations should establish a **"Regulatory Watch Process"** to systematically monitor, evaluate, and integrate new guidelines, delegated acts, and international standards into their internal governance structures.

This continuous scanning ensures early awareness of upcoming regulatory changes and alignment with evolving European and global frameworks.

© A4Q Copyright 2025

Adaptive Governance Structures

Future compliance models must be flexible and scalable.
Existing policies, roadmaps, and audit plans should be designed to incorporate new requirements—such as those emerging from AI Act 2.0, the Cyber Resilience Act, or revisions of ISO/IEC 42001—without disrupting established systems or workflows.

Interdisciplinary Cooperation

Forward-looking AI compliance relies on close collaboration between legal, IT, ethics, cybersecurity, and research departments.
These interdisciplinary structures enable organizations to anticipate and evaluate emerging risks—such as those related to *Frontier AI*, *autonomous decision-making*, or *cross-border data flows*.

Communication and Reporting

From 2026 onward, companies are expected to publish regular reports to management, supervisory bodies, and external stakeholders, covering AI-related risks, audit outcomes, and regulatory changes.
These reports enhance transparency, support liability prevention, and build long-term trust with regulators, investors, and the public.

Conclusion:
Strategic adaptability will become a core competency of AI governance.
Organizations that establish structures for regulatory learning early on will secure competitive advantages and minimize future compliance costs.

19.6 Recommended Focus Areas for Further Development (2025–2030)

For organizations and professionals aiming to go beyond the minimum legal requirements and prepare for future developments, the following areas of specialization are recommended:

- **Establishing an Internal AI Trend Radar:**
  Create an interdisciplinary team that annually analyzes technological, regulatory, and ethical trends, providing actionable insights and recommendations for management and compliance.
- **Participation in EU Consultations and Standardization Projects:**
  Engage actively in European and international standardization bodies such as CEN/CENELEC JTC 21 and ISO/IEC JTC 1/SC 42 to gain early insight into emerging standards, testing frameworks, and conformity assessment methods.
- **Networking with National AI Safety Initiatives:**
  Collaborate with national competence centers such as BAAIN (Germany), AIT (Austria), Fraunhofer IAO, VDE AI Quality & Testing Hub, or Swiss AI Lab IDSIA to conduct joint projects on AI safety, testing, and compliance.

© A4Q Copyright 2025

- **Exploring Future AI Ethics and Liability Issues:**
  Engage in research and training on emerging topics such as autonomous decision-making systems, moral responsibility in AI, the AI personhood debate, and ethical frameworks for self-learning agents.

These focus areas strengthen an organization’s ability to actively shape future developments and support Europe’s leadership in safe, responsible, and transparent AI governance.

© A4Q Copyright 2025

20 Recommendations for Training Providers

To ensure a consistent and practice-oriented learning experience within the A4Q AI Certified Compliance Training, it is recommended that training providers integrate at least one applied learning tool per chapter, such as a case study, checklist, mini-exercise, or template.

The concrete design will vary depending on the target group, industry context, and participants' experience level.
The goal of these recommendations is to strengthen the practical applicability of the syllabus content and ensure a sustainable transfer of knowledge into real-world organizational contexts.

Training providers are encouraged to use the following suggestions as a didactic guide when designing their training programs.
The selection, combination, and depth of practice examples may be adapted as needed – provided that the practical learning outcomes and content are consistent with the syllabus are maintained.

Chapter	Recommended Training Provider Deliverable	Purpose and Benefit for Participants
1 – Introduction to AI Compliance & the EU AI Act	Short self-assessment or discussion exercise: "Which role do I play under the AI Act?" (Provider, Deployer, etc.)	Strengthens role understanding and helps identify individual responsibilities.
2 – Risk-Based Approach & Classification	Mini-exercise on classifying use cases under Annex III, supported by a risk classification checklist.	Facilitates practical understanding of the risk-based approach.
3 – Global & Sectoral Regulatory Landscape	Comparative overview (EU – USA – China) with discussion guide on international differences.	Enhances global awareness and strategic decision-making skills.
4 – Prohibited AI Practices (Art. 5)	Short case scenario and decision task ("permitted or prohibited?").	Sharpens awareness of legal boundaries and ethical constraints.
5 – High-Risk Systems (Art. 6–51)	Example of a conformity dossier or checklist outlining CE process steps.	Connects legal requirements with operational implementation.
6 – Risk Management & QMS (ISO 42001 / 23894)	Sample AI risk register or ISO mapping sheet.	Demonstrates how to document and evaluate risks in practice.

© A4Q Copyright 2025

Chapter	Recommended Training Provider Deliverable	Purpose and Benefit for Participants
7 – Conformity Assessment & CE Marking	Process flow diagram of the CE procedure and example checklist (Art. 43–51).	Builds participant understanding of conformity assessment steps.
8 – Transparency Obligations & Limited-Risk Systems	Example of a transparency label (chatbot notice, deepfake disclosure) plus a UX compliance checklist.	Promotes user transparency awareness and trust-building.
9 – GPAI & Systemic Risk	Due diligence checklist for third-party models and sample supplier contract clauses.	Clarifies how to safely integrate external models and manage vendor risk.
10 – FRIA (Fundamental Rights Impact Assessment)	Template of a compact FRIA matrix with example evaluation.	Makes fundamental rights assessment directly applicable.
11 – Post-Market Monitoring & Incident Reporting	Example incident report form and simplified monitoring dashboard.	Strengthens understanding of monitoring and reporting obligations.
12 – Governance & Organizational Roles	Example RACI matrix and AI Officer role description.	Facilitates practical organizational implementation.
13 – Voluntary Governance & Ethics	Short reflection task or facilitation guide for an ethics workshop.	Encourages ethical awareness and CSR/ESG integration.
14 – Audit Readiness & Sanctions	Example self-audit questionnaire or maturity check.	Provides hands-on preparation for internal and external audits.
15 – Harmonized Standards & Norms	Mapping exercise: ISO 42001 ↔ AI Act, with annotations.	Illustrates the role and application of harmonized standards.
16 – International Interfaces & Export Control	Flowchart or decision tree for export and sanctions risk evaluation.	Supports risk assessment in international AI projects.
17 – Practice Exercises & Case Studies	Full exercise templates (Audit Plan, FRIA, Labeling Checklist).	Ensures practice-based learning and transferable skills.

© A4Q Copyright 2025

Chapter	Recommended Training Provider Deliverable	Purpose and Benefit for Participants
18 – Readiness Roadmap & Implementation	Template for an AI Act readiness roadmap with quick-win examples.	Simplifies the development of concrete implementation plans.
19 – Future Outlook & Regulatory Evolution	Discussion task: “Which upcoming developments affect my organization?”	Encourages forward-looking thinking and strategic foresight.

Summary:

By incorporating interactive, applied learning components, training providers help participants bridge the gap between theory and practice.

This approach fosters not only regulatory understanding but also the skills, confidence, and mindset needed to implement AI compliance effectively within organizations.

© A4Q Copyright 2025

21 Learning Objectives and Cognitive Learning Levels

Bloom's Taxonomy was first developed in 1956 by Benjamin Bloom and his team to systematically categorize learning objectives in the cognitive domain and create a common language for educational goals.
In 2001, Lorin W. Anderson and David R. Krathwohl fundamentally revised the model to better reflect modern learning and thinking processes.
In this revision, the stages were transformed into action-oriented verbs, and the highest level was redefined from *evaluation ("Evaluate")* to *creative production ("Create")*.

The revised taxonomy distinguishes six hierarchical levels (K1–K6) – from the recall of simple facts (K1), through understanding and application (K2, K3), to analysis (K4), evaluation (K5), and the creation of new concepts (K6).
This structure supports the precise formulation of learning objectives and examination requirements, particularly in dynamic fields such as Artificial Intelligence (AI), Data Protection (GDPR), and the regulation of AI systems under the EU AI Act.

Level	Designation	Description	Typical Verbs	Example Tasks
K1	Remember	Retrieve and reproduce facts, terms, and information accurately.	list, recall, identify, name	– "List the four risk categories of the EU AI Act." – "Name the core principles of the GDPR."
K2	Understand	Comprehend, interpret, and explain meanings and relationships.	explain, describe, summarize, interpret	– "Explain why AI systems are subject to different obligations under the EU AI Act." – "Describe the meaning of 'consent' under the GDPR."
K3	Apply	Use and implement knowledge in concrete situations.	apply, demonstrate, execute, use	– "Apply the EU AI Act criteria to determine the risk class of a chatbot." – "Apply GDPR requirements to draft a website privacy notice."
K4	Analyze	Break down information into components and identify relationships and structures.	analyze, differentiate, examine, compare	– "Analyze the differences between the regulation of high-risk AI systems under the EU AI

© A4Q Copyright 2025

Level	Designation	Description	Typical Verbs	Example Tasks
				Act and the GDPR.” – “Examine the connections between data security obligations in the AI Act and the GDPR.”
K5	Evaluate	Make judgments and critically assess arguments or methods.	evaluate, justify, critique, verify	– “Evaluate the effectiveness of the risk assessment requirements in the EU AI Act.” – “Critique the effectiveness of the GDPR in protecting personal data on social media platforms.”
K6	Create	Develop new products, theories, or solution approaches.	design, plan, conceptualize, generate	– “Design a concept for AI system development that fully complies with the EU AI Act.” – “Plan a data protection–compliant mobile app in accordance with the GDPR.”

This revised taxonomy provides educators and trainers with a structured framework for defining measurable learning objectives and designing progressive assessments, ensuring both knowledge acquisition and applied competence development.

© A4Q Copyright 2025

22 Literature

22.1 Professional Literature

[1] Thomas H. Davenport, Nitin Mittal, *All-in on AI: How Smart Companies Win Big with Artificial Intelligence*, Harvard Business Review Press, 2023 (Kap. 1, 2, 6, 12, 18)

[2] Ajay Agrawal, Joshua Gans, Avi Goldfarb, *Power and Prediction: The Disruptive Economics of Artificial Intelligence*, Harvard Business Review Press, 2022 (Kap. 1, 2, 3, 12, 19)

[3] Erik Brynjolfsson, Andrew McAfee, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*, W. W. Norton & Company, 2016 (Kap. 1, 13, 19)

[4] Luciano Floridi (ed.), *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities*, Oxford University Press, 2023 (Kap. 3, 8, 13, 15, 19)

[5] Andrew McAfee, Thomas H. Davenport, *The AI Advantage: How to Put the Artificial Intelligence Revolution to Work*, MIT Press, 2018 (Kap. 1, 2, 6, 12)

[6] Yuval Noah Harari, *Homo Deus: A Brief History of Tomorrow*, Harper, 2017 (Kap. 1, 13, 19)

[7] Max Tegmark, *Life 3.0: Being Human in the Age of Artificial Intelligence*, Penguin Books, 2018 (Kap. 13, 19)

[8] Pascal Finette, Jeffrey Rogers, *The Disruption Map: AI and the Future of Business*, Singularity University Press, 2022 (Kap. 1, 3, 12, 18, 19)

[9] Mark Coeckelbergh, *AI Ethics*, MIT Press, 2020 (Kap. 8, 13, 15, 19)

[10] Jacob Turner, *Robot Rules: Regulating Artificial Intelligence*, Palgrave Macmillan, 2019 (Kap. 3, 4, 5, 13, 15)

[11] Justin B. Bullock et al. (eds.), *The Oxford Handbook of AI Governance*, Oxford University Press, 2023 (Kap. 5, 6, 11, 12, 13, 15)

[12] Roger Brownsword et al. (eds.), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, Cambridge University Press, 2020 (Kap. 3, 4, 5, 13, 15, 16)

[13] Tshilidzi Marwala, Ebo Banjo Adam, *The Governance of Artificial Intelligence*, Elsevier, 2024 (Kap. 6, 11, 12, 15, 18)

[14] Janelle Shane, *You Look Like a Thing and I Love You: How AI Works and Why It's Making the World a Weirder Place*, Little Brown Spark, 2019 (Kap. 1, 2, 8)

[15] Kate Crawford, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, Yale University Press, 2021 (Kap. 3, 13, 16, 19)

[16] John C. Havens, *Heartificial Intelligence: Embracing Our Humanity to Maximize Machines*, TarcherPerigee, 2016 (Kap. 13, 19)

[17] Mazyar Peihani et al., *Principles of AI Governance and Model Risk Management*, Springer Nature, 2023 (Kap. 6, 7, 12, 14, 15)

[18] John Basl et al., *Governing the Machine: How to Navigate the Risks of AI and Unlock its True Potential*, MIT Press, 2024 (Kap. 6, 11, 12, 14, 18)

© A4Q Copyright 2025

[19] Patrick Lin, Keith Abney, Ryan Jenkins (eds.), *Robot Ethics 2.0: From Autonomous Cars to Artificial Intelligence*, Oxford University Press, 2017 (Kap. 8, 13, 16)
[20] George Musser, *Putting Ourselves Back in the Equation: Why Physicists Are Studying Human Consciousness and AI*, Farrar, Straus & Giroux, 2023 (Kap. 13, 19)
[21] John Zysman, Martin Kenney (eds.), *AI and the Boardroom: Corporate Governance, Strategy and Accountability in the Age of Artificial Intelligence*, Routledge, 2024 (Kap. 12, 13, 15, 18)
[22] Michael G. Solomon, *AI and Cybersecurity for Leaders*, CRC Press, 2023 (Kap. 6, 11, 16)
[23] National Institute of Standards and Technology (NIST), *AI Risk Management Framework – Generative AI Profile (NIST AI 600-1)*, U.S. Department of Commerce, 2024 (Kap. 6, 9, 11, 14, 15, 18)
[24] OECD, *AI Governance Principles and Implementation Guidance*, OECD Publishing, 2023 (Kap. 3, 12, 13, 15, 19)

22.2 Academic and Industry Reports

[1] McKinsey & Company, *The State of AI in 2024: Scaling Generative AI Responsibly*, McKinsey Global Report, 2024.
[2] Deloitte, *AI Governance in Practice: From Compliance to Competitive Advantage*, Deloitte Insights, 2024.
[3] Boston Consulting Group (BCG), *Bridging the Trust Gap: Responsible AI and Regulation in Europe*, BCG Report, 2024.
[4] PwC, *AI Regulation Monitor 2025: Implementing the EU AI Act in Practice*, PwC Global Study, 2025.
[5] EY, *The Future of Responsible AI: Balancing Innovation and Regulation*, EY Global AI Report, 2024.
[6] Accenture Research, *AI at Scale 2024: Operationalizing Trustworthy AI Systems*, Accenture Global Report, 2024.
[7] Capgemini Research Institute, *Generative AI and Responsible Use: Managing Ethics and Risk*, Capgemini Report, 2024.
[8] IBM Institute for Business Value, *Global AI Adoption Index 2024*, IBM Insights, 2024.
[9] National Institute of Standards and Technology (NIST), *AI Risk Management Framework – Generative AI Profile (NIST AI 600-1)*, U.S. Department of Commerce, 2024.
[10] OECD, *AI Policy Outlook 2024: Governance, Risk and Trust in Artificial Intelligence*, OECD Publishing, Paris, 2024.
[11] European Commission / AI Office, *Guidelines on Transparency and General-Purpose AI Models (Art. 53 AI Act)*, EU Official Publication, Brussels, 2025.
[12] European Commission / AI Office, *Draft Guidance on Serious AI Incidents and Post-Market Monitoring*, Consultation Draft, 2025.
[13] ENISA, *Threat Landscape for Artificial Intelligence 2025*, ENISA Report, Athens, 2025.
[14] World Economic Forum (WEF), *Global AI Governance Report 2024: Shaping Responsible AI Ecosystems*, WEF White Paper, Geneva, 2024.

© A4Q Copyright 2025

[15] Center for the Governance of AI (University of Oxford), *AI Governance Report 2025: Accountability and Global Standards*, Oxford Initiative on AI Ethics, 2025.
[16] NIST / U.S. Department of Commerce, *AI RMF Implementation Companion for Generative AI*, Gaithersburg, 2024.
[17] Stanford Institute for Human-Centered Artificial Intelligence (HAI), *Artificial Intelligence Index Report 2024*, Stanford University, 2024.
[18] Brookings Institution, *Advancing AI Accountability: Global Frameworks and Institutional Roles*, Brookings AI Policy Brief, 2024.
[19] World Bank, *AI for Development and Regulation: Building Trustworthy AI Ecosystems*, World Bank Group, Washington D.C., 2024.
[20] Gartner, *Top Trends in AI Governance, Risk and Compliance 2025*, Gartner Research Note, 2025.
[21] Microsoft / LinkedIn Economic Graph, *AI Skills and Jobs 2025: Global Workforce Readiness Report*, Microsoft Insights, 2025.
[22] OECD.AI Observatory, *AI Incidents Monitor 2025 – Learning from Real-World Failures*, OECD Policy Report, 2025.
[23] NIST & EU AI Office (Joint Workshop Summary), *Toward Harmonized AI Risk Management Frameworks*, Washington / Brussels, 2025.
[24] MIT Sloan Management Review, *Trust in AI: Strategies for Governance and Ethical Deployment*, MIT SMR Special Report, 2024.
[25] World Economic Forum, *Generative AI Governance Framework: Aligning Innovation and Accountability*, WEF White Paper, Geneva, 2025.

22.3 Legal Frameworks and Strategic Documents

[1] **Regulation (EU) 2024/1689** of 13 June 2024 – *Artificial Intelligence Act*, Official Journal of the EU L 2024/1689, 12 July 2024. ELI: data.europa.eu/eli/reg/2024/1689/oj.

[2] **Regulation (EU) 2016/679** – *General Data Protection Regulation (GDPR)*, effective since 25 May 2018.

[3] **Regulation (EU) 2023/2854** – *Data Act*, 13 December 2023 – Fair access and use of data.

[4] **Regulation (EU) 2022/2065** – *Digital Services Act (DSA)*, 27 October 2022 – Rules for digital services and platform responsibility.

[5] **Regulation (EU) 2022/1925** – *Digital Markets Act (DMA)*, 21 September 2022 – Competition rules for digital “gatekeeper” platforms.

[6] **Directive (EU) 2022/2555** – *NIS 2 Directive*, 27 December 2022 – High common level of cybersecurity across the EU.

[7] **Regulation (EU) 2019/881** – *Cybersecurity Act*, 7 June 2019 – Establishing ENISA and the EU Cybersecurity Certification Framework.

© A4Q Copyright 2025

[8] **Regulation (EU) 2024/2847** – *Cyber Resilience Act (CRA)*, 23 October 2024 – Horizontal cybersecurity requirements for digital products and software.

[9] **Regulation (EU) 2022/868** – *Data Governance Act (DGA)*, 3 June 2022 – Framework for data intermediation and trust services.

[10] **Directive (EU) 2024/2853** – *Product Liability Directive (Recast)*, 23 October 2024 – Modernisation of liability rules for software and AI; applicable from 9 December 2026.

[11] **Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (CETS No. 225)**, 5 September 2024 – First legally binding international AI treaty ("AIFC").

[12] **Directive (EU) 2025/…** – *AI Liability Directive* (expected adoption late 2025) – Harmonisation of civil liability rules for AI-related damage (replacing Proposal COM(2022) 496).

[13] **Spain – Royal Decree 817/2023** – *AI Regulatory Sandbox*, establishing test environments for high-risk AI systems within the EU AI Act implementation framework.

[14] **Spain – Draft Law for the Good Use and Governance of AI**, March 2025 – Complementing the EU AI Act with national rules on licensing and sanctions.

[15] **Spain – Spanish Agency for the Supervision of Artificial Intelligence (AESIA)**, established 2023 – First national AI supervisory authority in Europe, based in A Coruña.

[16] **Italy – National AI Strategy and Implementation Plan 2024–2026**, Ministry for Technological Innovation and Digital Transition (MITT) – Human-centric AI governance and innovation policy.

[17] **Netherlands – AI Governance Roadmap 2025**, National Strategy for EU AI Act Implementation with the Autoriteit Persoonsgegevens and accredited audit bodies.

[18] **United Kingdom – AI Regulation Bill (Draft 2025)** – Proposed UK framework introducing impact-assessment obligations and cross-sectoral governance requirements.

[19] **United Kingdom – Data (Use and Access) Act 2025**, adopted 19 June 2025 – Regulates access rights to training data for AI models and third-party providers.

[20] **United Kingdom – Product Regulation and Metrology Act 2025**, 21 July 2025 – Updating UK product safety and market surveillance laws for AI-based products.

[21] **OECD – Recommendation on Artificial Intelligence**, adopted 22 May 2019 – First intergovernmental AI policy framework for trustworthy AI.

[22] **UNESCO – Recommendation on the Ethics of Artificial Intelligence**, adopted 23 November 2021 – Global ethical framework for human-centric AI governance.

[23] **G7 – Hiroshima AI Process Code of Conduct for Advanced AI Systems**, endorsed October 2023 – Voluntary principles for Frontier AI safety and responsibility.

© A4Q Copyright 2025

[24] **United Nations – Global Digital Compact (Draft 2025)** – UN initiative on AI governance, data ethics, and sustainable digital development.

[25] **OECD – AI Governance Policy Observatory Reports 2025**, OECD Publishing, Paris – Comparative overview of national AI strategies and regulatory approaches.

22.4 International Standards and Technical Specifications

[1] **ISO/IEC 22989:2022**, *Artificial Intelligence – Concepts and Terminology*, International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC).

[2] **ISO/IEC 23053:2022**, *Framework for Artificial Intelligence (AI) Systems Using Machine Learning*, ISO/IEC JTC 1/SC 42.

[3] **ISO/IEC TR 24028:2020**, *Artificial Intelligence – Overview of Trustworthiness in AI*, ISO/IEC JTC 1/SC 42.

[4] **ISO/IEC 23894:2023**, *Artificial Intelligence – Guidance on Risk Management*, ISO/IEC JTC 1/SC 42.

[5] **ISO/IEC 42001:2023**, *Artificial Intelligence Management System (AIMS) – Requirements*, ISO/IEC JTC 1/SC 42.

[6] **ISO/IEC 42006:2025**, *Requirements for Bodies Auditing and Certifying Artificial Intelligence Management Systems (AIMS)*, ISO/IEC JTC 1/SC 42.

[7] **ISO/IEC 5259-1:2024**, *Data Quality for Analytics and Machine Learning – Part 1: Overview and Vocabulary*, ISO/IEC JTC 1/SC 42.

[8] **ISO/IEC 5259-2:2024**, *Data Quality for Analytics and Machine Learning – Part 2: Data Quality Model and Metrics*, ISO/IEC JTC 1/SC 42.

[9] **ISO/IEC 5259-4:2024**, *Data Quality for Analytics and Machine Learning – Part 4: Process Framework*, ISO/IEC JTC 1/SC 42.

[10] **ISO/IEC 5259-5:2025**, *Data Quality for Analytics and Machine Learning – Part 5: Data Governance*, ISO/IEC JTC 1/SC 42.

[11] **ISO/IEC 5338:2023**, *Artificial Intelligence – AI System Life Cycle Processes*, ISO/IEC JTC 1/SC 42.

[12] **ISO/IEC 38507:2022**, *Information Technology – Governance of IT – Governance Implications of the Use of Artificial Intelligence*, ISO/IEC JTC 1/SC 40.

[13] **ISO/IEC TR 24027:2021**, *Artificial Intelligence – Bias in AI Systems and AI-Aided Decision Making*, ISO/IEC JTC 1/SC 42.

[14] **ISO/IEC TR 24029-1:2021**, *Artificial Intelligence – Assessment of the Robustness of Neural Networks – Part 1: Overview*, ISO/IEC JTC 1/SC 42.

© A4Q Copyright 2025

[15] **ISO/IEC 24029-2:2023**, *Artificial Intelligence – Assessment of the Robustness of Neural Networks – Part 2: Formal Methods*, ISO/IEC JTC 1/SC 42.

[16] **ISO/IEC TR 29119-11:2020**, *Software Testing – Part 11: Testing of AI-Based Systems*, ISO/IEC JTC 1/SC 7.

[17] **ISO/IEC 25059:2023**, *Systems and Software Quality Requirements and Evaluation (SQuaRE) – Quality Model for AI Systems*, ISO/IEC JTC 1/SC 7.

[18] **ISO/IEC 27001:2022**, *Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements*, ISO/IEC JTC 1/SC 27.

[19] **ISO/IEC 27701:2019**, *Security Techniques – Extension to ISO/IEC 27001 for Privacy Information Management – Requirements and Guidelines*, ISO/IEC JTC 1/SC 27.

22.5 International AI Ethics and Governance Frameworks

[1] **NIST AI Risk Management Framework – Generative AI Profile (NIST.AI.600-1, 2024)** – A specialized profile of the U.S. National Institute of Standards and Technology (NIST) AI RMF focusing on risks, controls, and evaluation methods for generative AI systems.

[2] **OECD Recommendation on Artificial Intelligence (OECD AI Principles, 2019)** – First intergovernmental, values-based policy framework promoting human-centered, transparent, and accountable AI; adopted by over 50 countries.

[3] **UNESCO Recommendation on the Ethics of Artificial Intelligence (2021)** – Global ethical standard adopted by UNESCO Member States, emphasizing human rights, transparency, inclusiveness, and sustainability in AI governance.

[4] **EU High-Level Expert Group on AI – Ethics Guidelines for Trustworthy AI (2019)** – Defines seven key requirements for trustworthy AI: human agency, technical robustness, privacy, transparency, fairness, societal well-being, and accountability.

[5] **IEEE 7000 Series / Ethically Aligned Design (EAD)** – A suite of IEEE standards and frameworks (e.g., IEEE 7000, 7001–7009) providing practical guidance on embedding ethical values into the design and development of AI and autonomous systems.

[6] **UN Global Digital Compact (Draft 2025)** – A forthcoming United Nations framework promoting safe, inclusive, and rights-based digital and AI governance worldwide, aligned with the UN 2030 Agenda for Sustainable Development.

© A4Q Copyright 2025

22.6 Cybersecurity Threat Landscape (AI Context)

[1] **ENISA Threat Landscape 2025 – Annual Report on the Threat Landscape (July 2024 – June 2025)**, European Union Agency for Cybersecurity (ENISA), 2025.
Comprehensive EU-wide overview of cyberthreats, highlighting AI-enabled attacks such as deepfakes, generative phishing, data poisoning, and LLM abuse.

[2] **ENISA AI Cybersecurity Challenges Report 2024**, ENISA, 2024.
Analysis of security risks in AI architectures and models, including adversarial attacks, model poisoning, and vulnerabilities in generative systems.

[3] **Europol / Trend Micro / UNICRI – Malicious Uses and Abuses of Artificial Intelligence: 2024 Update**, 2024.
Joint report on criminal exploitation of AI technologies – deepfakes, voice cloning, automated fraud, and misinformation campaigns.

[4] **NIST Cybersecurity Framework (CSF 2.0, 2024)**, U.S. Department of Commerce / NIST, 2024.
Updated framework integrating AI-related security guidance and mappings to the NIST AI RMF and ISO/IEC 27001 standards.

[5] **World Economic Forum (WEF) – Global Cybersecurity Outlook 2025**, WEF, 2025.
Focus on generative-AI risks, supply-chain threats, and manipulation of critical information infrastructure at a global scale.

[6] **Microsoft Digital Defense Report 2024**, Microsoft Corporation, 2024.
Annual analysis of global cyberthreats, including AI-driven disinformation, automated malware generation, and nation-state operations.

[7] **Google / Mandiant Threat Intelligence Report 2025**, Google Cloud / Mandiant, 2025.
Insights into AI-assisted exploitation techniques such as prompt injection, automated vulnerability scanning, and malicious code generation.

[8] **Europol – Internet Organised Crime Threat Assessment (IOCTA 2025)**, Europol, 2025.
EU law enforcement report on AI-enabled cybercrime, automated attacks, and emerging fraud schemes using machine learning tools.

[9] **OECD / ENISA Joint Policy Brief 2025 – AI Safety & Cyber Resilience**, OECD Publishing / ENISA, 2025.
Policy guidance for member states on security-by-design principles, incident information sharing, and cross-border coordination for AI safety.

© A4Q Copyright 2025

23 Appendices

23.1 Appendix A – International Provider Guidance

Guidance for Providers Outside the EU Offering AI Systems Within the EU, and for Providers Operating in Other Jurisdictions with Different Regulatory Approaches

International Addendum – A4Q AI Certified Compliance Officer Syllabus

Chapter	Focus (Topic)	Obligations / Particularities for Non-EU Providers	Recommended Measures / Tools
1	Introduction & Scope	Extraterritorial scope of the AI Act: Providers outside the EU are subject to it if their system is used within the EU.	Appoint an EU representative; prepare CE conformity; document EU legal applicability.
2	Risk-based Approach	Adopt EU risk categories to enable product comparability and compliance evidence.	Map risk levels to NIST AI RMF (US) or AIDA (Canada).
3	Global Regulatory Landscape	Diverse AI laws: US (NIST), UK (Principles-based), China (Generative AI Rules), Brazil (Marco Legal AI), Canada (AIDA).	Maintain a “Global Regulatory Matrix”; add local regulatory modules.
4	Risk Management & Technical Compliance	Combine risk management frameworks from ISO/IEC 23894 and NIST AI RMF.	Maintain a unified risk register; harmonize global risk categories.
5	Data Quality & Governance	Non-EU data must meet GDPR-equivalent safeguards.	Conduct Data Transfer Impact Assessments (DTIA); apply Standard Contractual Clauses; ensure verifiable data provenance.
6	Technical Documentation	EU requires a Technical File as per Annex IV AI Act.	Establish a global “AI Conformity Dossier”; reference Model Cards and Data Sheets.

© A4Q Copyright 2025

Chapter	Focus (Topic)	Obligations / Particularities for Non-EU Providers	Recommended Measures / Tools
7	Transparency & Labeling	Disclosure obligations vary (EU Art. 52, China Labeling, US voluntary).	Implement a multi-label system for AI outputs and usage disclosures.
8	Human Oversight & Safety	EU mandates “Human Oversight”; US/NIST emphasize “Responsible Human Participation.”	Conduct training and maintain checklists for human-in-the-loop control.
9	General-Purpose AI & Foundation Models	EU Arts. 53–55 define GPAI obligations; US NIST and UK frameworks require documentation and safety testing.	Use GPAI compliance templates; create Model Evaluation Reports.
10	Fundamental Rights Impact Assessment (FRIA)	EU FRIA parallels US/Canada “Algorithmic Impact Assessments.”	Apply a unified impact-assessment template (compatible with EU and AIDA requirements).
11	Post-Market Monitoring	Incident reporting must also be performed by non-EU providers toward EU authorities.	Implement PMS processes (ISO/IEC 42001); establish a shared reporting channel with EU partners.
12	Governance & Internal Roles	EU requires an AI Officer; other regions use AI Governance Boards or Responsible AI Leads.	Set up a global AI Governance Board; define and document accountability.
13	Voluntary Governance & Ethics	OECD, UNESCO, and G7 Codes of Conduct, recognized as global ethical frameworks.	Embed an AI ethics code within the organization; consider voluntary certification (e.g., NIST or IEEE).
14	Audit & Evidence Management	EU compliance must be auditable; US NIST encourages internal audits; the UK uses an “Assurance Framework.”	Conduct internal/external AI audits (ISO/IEC 42001, 27001).
15	Harmonized Standards	EU “Presumption of Conformity” achievable via ISO/IEC standards.	Apply ISO/IEC 42001, 23894, 22989, 23053; maintain a standards library.

© A4Q Copyright 2025

Chapter	Focus (Topic)	Obligations / Particularities for Non-EU Providers	Recommended Measures / Tools
16	Export Control & Supply Chains	Comply with EU Dual-Use Regulation, US ITAR/EAR, and China's technology export laws.	Verify export classification; document a global compliance chain.
17	Practical Implementation & GPAI Management	Establish a unified global documentation structure for GPAI and FRIA processes.	Harmonize AI compliance templates across the EU, US, and China.
18	Roadmap & Readiness	Compare maturity levels across the EU AI Act, NIST, and AIDA frameworks.	Conduct global AI readiness assessments; implement a maturity model.
19	Future Trends & International Convergence	Increasing alignment is expected among the EU, US, OECD, and G7 jurisdictions.	Participate in ISO/IEC SC 42 and CEN/CENELEC JTC 21; plan a global certification strategy.

General Recommendation for International Providers

- **Establish a Compliance Hub:** Central repository covering all key jurisdictions (EU, US, UK, China, Canada, Brazil).
- **Maintain Dual Documentation:** Keep EU AI Act dossiers + US NIST profiles in parallel.
- **Develop a Global Certification Strategy:** Use ISO/IEC 42001 as a common compliance layer across markets.
- **Legal Monitoring:** Implement early-warning systems for delegated acts and emerging national AI bills.

© A4Q Copyright 2025