
# Navigating the Future of Responsible AI

## How the EU AI Act, ISO 42001 and GDPR Converge

May 2026

# Artificial Intelligence is transforming industries, accelerating innovation, and redefining how organisations operate. But with this transformation comes heightened regulatory scrutiny and the need for responsible, transparent and well-governed AI ecosystems.

The risks of deploying AI without robust governance are no longer theoretical—they are operational, legal, and societal. Poorly governed AI systems can entrench bias, discriminate at scale, compromise privacy, and make opaque decisions that cannot be explained or challenged. When AI models are trained or deployed without clear accountability, data discipline, or human oversight, organizations risk automating harm faster than they can detect or correct it. Beyond individual impact, irresponsible AI erodes public trust in digital systems, undermines confidence in innovation, and fuels regulatory backlash that can slow adoption even for well-intentioned actors.

The consequences for organisations are equally severe. Regulatory penalties, litigation, forced withdrawal of AI systems, and reputational damage can far outweigh the short-term gains of rapid experimentation without controls. As AI becomes embedded in core business processes—credit decisions, hiring, healthcare, security, and public services—failures are no longer isolated technical incidents but enterprise-level risk events. In this context, responsible AI is not a compliance afterthought or ethical aspiration; it is a prerequisite for sustainable AI value creation. Regulations and standards now formalize this expectation, signalling a shift from voluntary best practices to enforceable accountability across the AI lifecycle.

Against this backdrop, responsible AI is no longer defined by intent alone but by the ability to demonstrate structured governance, risk control and legal compliance across the AI lifecycle. This expectation is now crystallising through a number of regulatory and standards-based frameworks that, when viewed together, translate ethical principles into enforceable requirements and operational practice. It is at this point that the convergence of regulation and standards becomes most visible.

Three frameworks now shape the new AI landscape:

- **The EU AI Act**
  The world's first comprehensive AI regulation
- **ISO 42001**
  The global standard for AI Management Systems (AIMS)
- **The GDPR**
  The foundational regulation governing the processing of personal data

Each framework addresses different aspects of trust, risk and accountability. Together, they form a comprehensive AI Compliance & Governance Operating Model (AI-CGOM) for building and deploying AI safely, lawfully and ethically.

As organisations accelerate their adoption of artificial intelligence, they face a governance landscape anchored by three complementary pillars. The EU AI Act establishes the legal obligations and risk-based requirements necessary to protect fundamental rights and ensure safe AI deployment. ISO 42001 provides the operational blueprint for implementing those obligations through a structured, auditable AI Management System. Meanwhile, the GDPR ensures that any personal data used within AI systems is processed lawfully, ethically and transparently.

When combined, these frameworks give organisations a clear path to building AI systems that are compliant by default, trustworthy by design and aligned with societal expectations.

## AI Compliance & Governance Operating Model

**Grant Thornton stands at the forefront of helping organisations navigate, operationalise and embed these requirements into a unified AI governance architecture.**

# 01 The New AI Regulatory Landscape

## The EU AI Act – A Risk-Based Legal Framework

The Act classifies AI systems based on risk (Unacceptable - Prohibited Use, High-Risk, Limited-Risk, Minimal-Risk), requiring organisations to implement strict controls for high-risk systems, including:

- Risk management
- High-quality, representative datasets
- Technical documentation and traceability
- Human oversight
- Logging and monitoring
- Transparency and explainability
- Post-market monitoring

It imposes obligations on both Providers and Deployers of AI systems.

Beyond its risk classifications, the EU AI Act introduces a comprehensive regulatory architecture designed to strengthen accountability and protect fundamental rights across the AI lifecycle. It establishes clear obligations for every actor in the AI value chain — Providers, Deployers, Importers, Distributors, and Product Manufacturers — ensuring that responsibility is shared and traceable. High-risk AI systems must undergo conformity assessments, be registered in an EU database, and maintain continuously updated technical documentation demonstrating compliance.

The Act also embeds fundamental rights protections through requirements such as Fundamental Rights Impact Assessments (FRIAs) for deployers in the public sector and imposes strict prohibitions on harmful or manipulative AI practices such as social scoring, behavioural manipulation, emotion recognition in workplaces and education, and indiscriminate biometric surveillance. Importantly, the regulation creates strong enforcement mechanisms, including substantial administrative fines, CE-marking obligations, post-market monitoring duties, and incident reporting requirements.

As a result, the EU AI Act not only sets the global benchmark for trustworthy and responsible AI but also demands that organisations adopt structured governance systems ensuring safety, transparency, fairness and ongoing oversight throughout the AI lifecycle.

## ISO 42001 – The Operational Backbone of AI Governance

Where the EU AI Act defines the legal parameters of acceptable AI, ISO 42001 operationalises these expectations into a management system that organisations can embed into daily practice. It introduces policies, procedures and lifecycle controls that ensure AI systems are developed, deployed and monitored consistently and safely. ISO 42001 is not a regulation but a governance framework — meaning it provides the "how" behind compliance, risk reduction and accountability.

ISO 4200 introduces the world's first AI Management System Standard. Where the EU AI Act defines the legal obligations, ISO 42001 defines how to operationalise them through:

- AI governance structures
- Policy, process and lifecycle controls
- AI system impact assessment
- AI risk management methodology
- Dataset governance and model documentation
- Explainability and transparency measures
- Monitoring, incident handling and continuous improvement

It provides a repeatable, auditable system aligned with the structure of other International Standards such as ISO 27001 (Information Security Management System - ISMS) and ISO 27701 (Privacy Information Management System - PIMS).

## GDPR – Ensuring Lawful and Ethical Data Use

While the EU AI Act governs the behaviour of AI systems and ISO 42001 governs how organisations manage them, GDPR governs the personal data flowing through those systems. It remains one of the most critical pillars of AI governance. Any AI model that processes personal data — during training, inference or monitoring — must comply with GDPR's strict principles of fairness, transparency, lawfulness and accountability. Organisations cannot achieve AI compliance without embedding GDPR safeguards into every stage of the AI lifecycle.

As many AI systems rely on personal data, the GDPR remains fully applicable.

- AI governance must incorporate:
- Lawful basis and purpose limitation
- Transparency to data subjects
- Data minimisation
- Safeguards for automated decision-making
- DPIAs for high-risk processing
- Accountability and documentation obligations

GDPR, therefore, governs how personal data flows into and through AI systems.

# 02 How These Frameworks Complement Each Other

While each framework has its own focus, together they are deeply interconnected.

| Framework | Primary Focus | How It Contributes to AI Governance |
|---|---|---|
| EU AI Act | Legal obligations, risk categories, controls for high-risk AI | Defines what organisations must do |
| ISO 42001 | Management system, processes, governance, lifecycle | Defines how to do it effectively and consistently |
| GDPR | Personal data protection, transparency, lawful processing | Ensures AI systems process data responsibly |

## EU AI Act, ISO/IEC 42001 & GDPR Mapping

| Theme/ Control Area | EU AI Act | GDPR | ISO 42001 Clauses | ISO 42001 Annex A Controls |
|---|---|---|---|---|
| Risk management and impact assessment | **Art. 9** \| Risk management system<br>**Art. 27** \| Fundamental rights impact assessment<br>**Art. 72** \| Post-market monitoring<br>**Art. 73** \| Serious incident reporting | **Art. 24** \| Responsibility of controller<br>**Art. 25** \| Data protection by design and by default<br>**Art. 32** \| Security of processing<br>**Art. 35** \| Data protection impact assessment | **6.1.1–6.1.3** \| AI risk assessment and treatment;<br>**6.1.4 & 8.4** \| AI system impact assessment;<br>**9.1** \| Monitoring and evaluation | **A.5.2–A.5.5** \| AI system impact assessment and documentation;<br>**A.6.2.4** \| Verification and validation;<br>**A.9.2** \| Processes for responsible use |
| Data and data governance | **Art. 10** \| Data and data governance for high-risk AI; Annex IV & VIII – Technical documentation and registration info on data and logic | **Arts. 5–6** \| Core data protection principles and lawful basis;<br>**Arts. 13–14** \| Information duties;<br>**Art. 25** \| Privacy by design;<br>**Art. 30** \| Records of processing activities | **4.1** \| Context including applicable data rules;<br>**6.1** \| Risk criteria including data;<br>**7.5** \| Documented information management | **A.4.3–A.4.5** \| Data, tooling and computing resources;<br>**A.7.2–A.7.6** \| Data management, quality, provenance, preparation |

| Theme/ Control Area | EU AI Act | GDPR | ISO 42001 Clauses | ISO 42001 Annex A Controls |
|---|---|---|---|---|
| Technical documentation and traceability | **Art. 11** \| Technical documentation; Annex IV – Content of technical documentation;<br>**Art. 47** \| EU declaration of conformity; Annex V – Content of the declaration | **Arts. 24 & 30** \| Documentation of measures and processing activities;<br>**Art. 35** \| Documentation of DPIAs | **7.5** \| Creation, update and control of documented information;<br>**8.1** \| Operational planning and control | **A.5.3** \| Documentation of impact assessments;<br>**A.6.2.3** \| Design and development documentation;<br>**A.6.2.7** \| AI system technical documentation |
| Logging, monitoring and post-market activity | **Art. 12** \| Record-keeping and logging;<br>**Art. 19** \| Retention of logs;<br>**Art. 72** \| Post-market monitoring; Art. 73 – Serious incident reporting | **Art. 5(2)** \| Accountability principle;<br>**Art. 30** \| Records of processing;<br>**Art. 33** \| Personal data breach notification | **8.1** \| Operational controls;<br>**9.1** \| Monitoring, measurement, analysis and evaluation | **A.6.2.6** \| Operation and monitoring;<br>**A.6.2.8** \| Recording of event logs;<br>**A.8.4** \| Incident communication to users |
| Human oversight and governance | **Art. 4** \| AI literacy;<br>**Art. 14** \| Human oversight;<br>**Arts. 16–26** \| Obligations of providers, importers, distributors and deployers of high-risk AI | **Art. 5** \| Core principles incl. fairness and accountability;<br>**Art. 22** \| Automated decision-making safeguards;<br>**Arts. 24–25** \| Governance and "by design" obligations | **5.1–5.3** \| Leadership, AI policy, roles and responsibilities;<br>**7.2–7.3** \| Competence and awareness | **A.3.2** \| AI roles and responsibilities;<br>**A.6.1.2** \| Objectives for responsible development;<br>**A.9.3–A.9.4** \| Objectives and controls for responsible and intended use |
| Transparency and information to users | **Art. 13** \| Transparency and instructions for use;<br>**Art. 50** \| Transparency for certain AI systems;<br>**Art. 86** \| Right to explanation of AI-supported decisions | **Arts. 12–15** \| Transparent, fair information and access rights;<br>**Art. 22(3)** \| Right to obtain explanation and human intervention in automated decisions | **7.4** \| Internal and external communication;<br>**8.1** \| Operational communication duties | **A.8.2** \| System documentation and information for users;<br>**A.8.5** \| Information duties towards interested parties |

| Theme/ Control Area | EU AI Act | GDPR | ISO 42001 Clauses | ISO 42001 Annex A Controls |
|---|---|---|---|---|
| Quality management and conformity | **Art. 17** \| Quality management system;<br>**Art. 41** \| Common specifications;<br>**Art. 43** \| Conformity assessment;<br>**Arts. 47–49** \| EU declaration, CE marking, registration | **Arts. 24, 25, 32** \| Organisational and technical measures, security and "by design" quality of processing | **4.4** \| AI management system;<br>**6.2** \| AI objectives;<br>**9.2–9.3** \| Internal audit and management review;<br>**10.1–10.2** \| Continual improvement and corrective action | **A.2.2–A.2.4** \| AI policy and review;<br>**A.6.1.3** \| Processes for responsible design and development;<br>**A.10.2–A.10.3** \| Allocation of responsibilities and supplier management |
| Security, robustness and resilience | **Art. 15** \| Accuracy, robustness and cybersecurity of high-risk AI | **Art. 5(1)(f)** \| Integrity and confidentiality;<br>**Art. 32** \| Security of processing | **6.1** \| Risk criteria including security;<br>**7.1** \| Resources;<br>**8.1** \| Operational control | **A.4.2–A.4.6** \| Resource documentation incl. systems and people;<br>**A.6.2.6** \| Operation and monitoring |
| Prohibited / unacceptable AI practices | **Arts. 5–7** \| Prohibited AI practices and classification rules for high-risk systems | **Arts. 5, 9–10** \| Principles, special categories and limitations on certain processing practices | **4.1** \| Context incl. prohibited uses;<br>**6.1.1** \| Defining AI risk criteria | **A.6.1.2** \| Objectives for responsible development;<br>**A.9.3** \| Objectives for responsible use |
| Fundamental rights, fairness and non-bias | **Recitals and Art. 10(3)** \| Data quality and representativeness; Art. 14 – Human oversight; Art. 27 – Fundamental rights assessment | **Arts. 5(1)(a)** \| Lawfulness, fairness, transparency;<br>**Arts. 6, 9** \| Legal bases & special-category safeguards | **4.2** \| Needs and expectations of interested parties;<br>**6.1.4** \| AI system impact assessment | **A.5.4–A.5.5** \| Impacts on individuals and society;<br>**A.7.4** \| Data quality requirements |
| Rights of affected persons / data subjects | **Art. 86** \| Right to an explanation of individual decision-making by deployers | **Arts. 12–15** \| Information and access;<br>**Arts. 16–18** \| Rectification, erasure, restriction;<br>**Art. 21–22** \| Objection and profiling | **4.2** \| Interested parties;<br>**7.4** \| Communication;<br>**8.1** \| Operational communication | **A.8.2** \| System documentation for users;<br>**A.8.3** \| External reporting channels |

| Theme/ Control Area | EU AI Act | GDPR | ISO 42001 Clauses | ISO 42001 Annex A Controls |
|---|---|---|---|---|
| Third-party, supplier and value-chain roles | **Arts. 16–26** \| Obligations of providers, importers, distributors, deployers and product manufacturers;<br>**Art. 25** \| Responsibilities along value chain | **Art. 28** \| Processor obligations;<br>**Arts. 26–29** \| Joint controllers and persons acting under authority | **4.1 & 4.3** \| Context and scope incl. roles;<br>**5.3** \| Roles, responsibilities, authorities | **A.10.2** \| Allocating responsibilities;<br>**A.10.3** \| Supplier management;<br>**A.3.3** \| Reporting concerns |
| Innovation, sandboxes and continuous improvement | **Arts. 53–55, 89** \| General-purpose models obligations and monitoring/supervision mechanisms | **Art. 24** \| Ongoing review of measures;<br>**Art. 32(1)** \| Regular testing and evaluation of effectiveness | **9.1** \| Monitoring and evaluation;<br>**9.2–9.3** \| Internal audit and management review;<br>**10.1** \| Improvement | **A.6.2.6** \| Ongoing monitoring;<br>**A.8.3** \| External feedback channels;<br>**A.2.4** \| Review of AI policy |

# 03 The GT AI Compliance & Governance Operating Model

Organisations that integrate these three frameworks create a governance architecture that is:

**Accountable** | **Transparent** | **Secure** | **Ethical** | **Regulatory-ready**

## The unified model includes

### AI Governance & Oversight

Establishes the organisational structures, roles, and decision-making mechanisms needed to manage AI responsibly. Ensures accountability, ethical alignment, and oversight at every stage of the AI lifecycle. Provides leadership visibility and control over AI initiatives.

### AI Risk Management

Identifies, evaluates, and mitigates risks associated with AI models, including bias, safety, transparency, security, and societal impact. Integrates both EU AI Act risk processes and ISO 42001 methodologies for structured, repeatable assessments. Maintains a proactive risk posture throughout deployment and operation.

### Data Governance & Data Protection

Ensures AI models use lawful, high-quality, representative, and ethically sourced data. Embeds GDPR compliance through minimisation, transparency, and data rights safeguards. Manages data lineage, quality, privacy, and integrity across training, testing, and inference.

### Model Lifecycle Management

Governs the end-to-end lifecycle of AI systems—from design and development to deployment, monitoring, and retirement. Standardises procedures for testing, validation, explainability, robustness, and model updates. Ensures ongoing compliance with regulatory and organisational requirements.

### Technical Assurance

Provides independent testing and validation of model behaviour, robustness, fairness, and security. Verifies that AI systems operate reliably under diverse conditions and are resistant to adversarial manipulation. Supports certification readiness and builds trust in outcomes.

### Logging, Monitoring & Post-Market Activities

Implements consistent logging, telemetry, and monitoring across AI systems to detect performance drift, anomalies, and risks. Supports EU AI Act post-market monitoring obligations and enables early corrective actions. Ensures AI behaviour remains aligned with expectations and regulatory requirements.

### Documentation & Audit Readiness

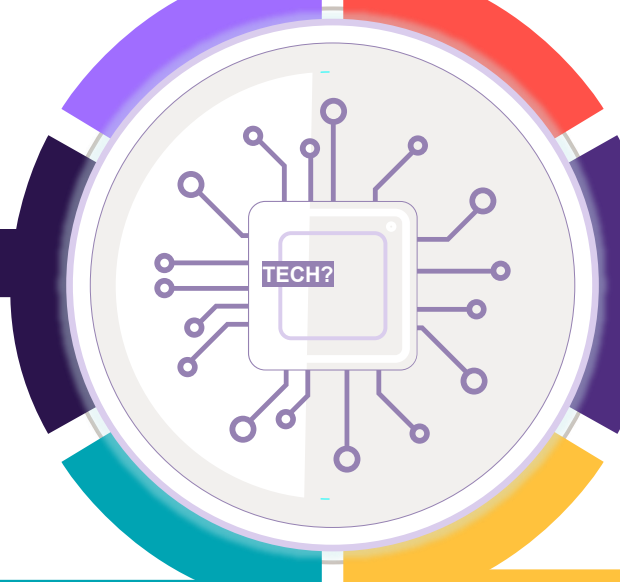
Maintains comprehensive, up-to-date technical and governance documentation demonstrating compliance with EU AI Act, ISO 42001, and GDPR. Ensures auditability through structured evidence, traceability, and version-controlled artefacts. Facilitates internal and external assessments with confidence.

### Continuous Improvement & AI Literacy

Promotes ongoing enhancement of AI processes, controls, and governance based on monitoring insights, incidents, and evolving regulations. Strengthens organisational AI literacy through training, awareness, and capability building. Ensures the organisation remains resilient and future-ready in a rapidly changing AI landscape.

This creates a scalable foundation for innovation while maintaining compliance and trustworthiness.

# How Grant Thornton Supports Organisations on the AI Compliance & Governance Journey




## EU AI Act Readiness & Implementation

- Identification and classification of all AI systems
- Internal Audit / Gap assessment against EU AI Act Articles 9–61
- Obligations roadmap for providers & deployers
- Preparation of technical documentation & conformity evidence

## Technical AI Assurance

- AI Model Audit & Testing
- Offensive Information Security – Penetration Testing
- Security and model governance checks
- AI Development Lifecycle testing

## ISO 42001 Implementation & Maintenance

- Design and build of the AI Management System (AIMS)
- Development of all policies, procedures, registers and templates
- Integration with existing ISO 27001 and ISO 27701 frameworks
- Internal audits and certification preparation
- Virtual AI Officer - Strategy, Development, and Ethical implementation

## AI Governance Operating Model

- Establishment of AI steering committee
- AI Policies and Procedures
- Virtual AI Officer
- Definition of responsibilities (AI Owner, AI Risk Manager, Ethical AI Lead)
- Escalation, reporting, and monitoring structures
- Integration with corporate governance frameworks

## GDPR and Data Protection for AI

- DPIAs specifically tailored for AI and automated decision-making
- Transparency & lawful basis assessments
- Personal data flows and minimisation techniques
- Privacy-by-design built across AI lifecycle
- Virtual DPO (vDPO) Services

Read more on our Privacy and Data Protection capabilities here

## AI Awareness, Literacy & Culture

- Executive briefings
- Training for auditors, risk teams and end users
- Awareness campaigns
- Practical workshops on ethical and trustworthy AI

# Why chose Grant Thornton

### Holistic Expertise

Regulatory, technical, operational and assurance capabilities under one roof

### Global Experience

Supporting clients across industries and jurisdictions

### Practical Execution

Not policy-heavy — focused on implementable solutions

### Future-Proofing

Helping organisations prepare for upcoming regulations and certifications

### Trusted Partner

A recognised leader in governance, risk, compliance and emerging technologies

Grant Thornton empowers organisations to adopt AI confidently, responsibly and competitively—transforming regulatory obligations into a strategic advantage.


References:

1. REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)
2. ISO/IEC 42001 (2023) – Artificial Intelligence Management System
3. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
4. EU AI Act Compliance Matrix - By IAPP Principal Researcher, Privacy Law and Policy, Müge Fazlioglu, CIPP/E, CIPP/US

# Contacts


**Christos Makedonas**
Partner, Digital Risk Services Leader
christos.makedonas@cy.gt.com

**Anna Papaonisiforou**
Senior Manager, GRC Services
anna.papaonisiforou@cy.gt.com

**Monica Odysseos**
Senior Manager, AI & Data Lab Leader
monica.odysseos@cy.gt.com

**Simon Loizides**
Principal, Offensive Security Services
simon.loizides@cy.gt.com

**Stavros Demetriou**
Senior Manager, Data Protection Services
stavros.demetriou@cy.gt.com

**Nicolas Markitanis**
Principal, Offensive Security Services
nicolas.markitanis@cy.gt.com

**Marios Nicolaides**
Principal, Offensive Security Services
marios.nicolaides@cy.gt.com


Grant Thornton