Gartner

Gartner for Legal, Risk & Compliance

An EU AI Act Readiness Checklist for Legal, Compliance, Risk and Audit

The EU AI Act will place new transparency, consent and disclosure obligations on organizations, while restricting high-risk uses of AI. With enforcement of some provisions looming, assurance leaders must start preparing for compliance now.

Overview

Key Findings

- The European Union AI Act (the Act) places new compliance obligations on deployers and developers of AI that operate in the EU.
- EU AI Act compliance requires changes to AI governance and oversight, risk assessment, monitoring and auditing, and policies, procedures and training.
- Assurance leaders must partner with the board and senior leaders to achieve compliance by removing or preventing prohibited uses of AI and mitigating the impact of high-risk AI use cases.

Recommendations

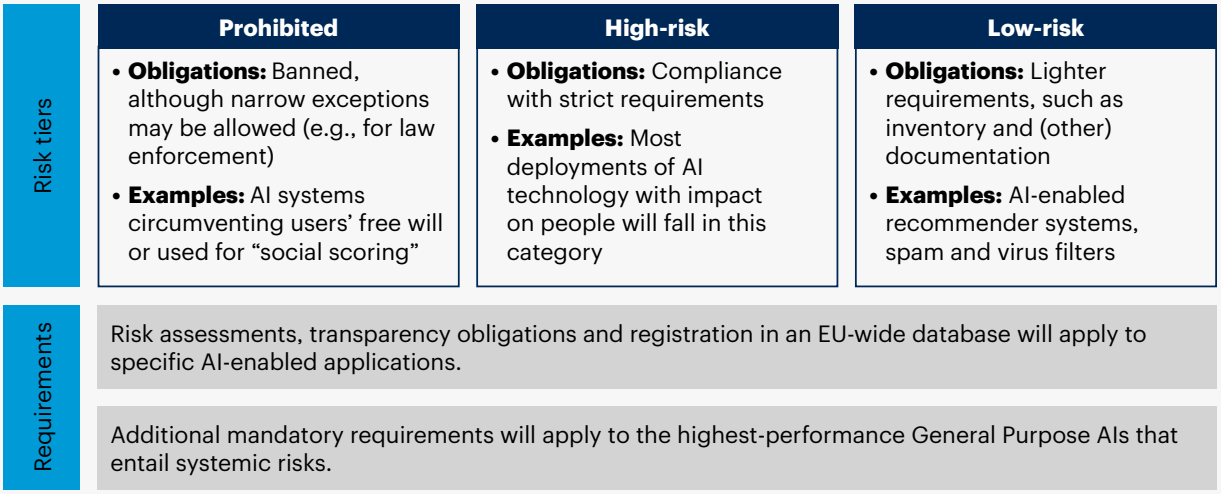
Assurance leaders should begin EU AI Act compliance efforts by:

- Communicating regulatory changes to senior leadership stakeholders now to minimize potential pushback for upcoming EU AI Act-required business process, projects and AI-systems assessments.
- Shortening the time to compliance by leveraging existing privacy and security risk management processes, policies and other resources that can or must be adapted to meet new EU AI Act requirements.
- Defining clear roles and responsibilities between legal, compliance, enterprise risk management and audit to establish ownership in the execution of AI governance and risk management processes.

New Risk-Based Requirements for AI Use

On 9 December 2023, the European Union Council presidency and the European Parliament reached a provisional agreement on a bill for the European Union AI Act (the Act). [1] The Act provides a comprehensive "risk-based" approach to AI regulation. It imposes different levels of restrictions on use cases based on the level of risk they pose, and also prohibits certain use cases altogether (see Figure 1). Additionally, the Act expands upon existing legal obligations like the General Data Protection Regulation (GDPR) and places new transparency obligations on enterprises using or developing Generative AI and General Purpose AI systems (GPAI).

Figure 1: Risk Categories in EU AI Act



Source: Gartner

Once finalized, the Act will apply to public and private sector organizations based in the EU as well as organizations operating in — but not based in — the EU. While formal adoption by the EU Parliament and Council is still pending, enforcement of some provisions will begin as soon as six months after the law's passage. Most of the remaining provisions will go into force two years after passage. [2]

Noncompliant Organizations Will Have to Pay Sizable Penalties

The Act entails a progressive sanctioning scale, which determines fines bound to the severity of the violations. The financial penalties will be expressed as a specific amount or a significant percentage of global annual turnover (up to 7% of the total worldwide annual revenue of the preceding financial year for the most egregious of violations).[3] Small-to-midsize businesses (SMBs) and startups will likely be fined in a way that is proportional to their size compared to larger technology firms. Since the Act builds upon the GDPR and similar privacy obligations, it is possible that transgressors could be fined for both a violation of the Act and the GDPR contemporaneously.

Assurance Leaders Must Begin Acting Now to Achieve Compliance

With enforcement and potential financial penalties on the horizon, assurance leaders — legal, compliance, privacy, risk and audit roles — must start taking action now to build a path toward compliance and assurance. However, the wide scope of new obligations posed by the EU AI Act and the cross-functional nature of AI strategy and implementation leave assurance leaders unsure of the role their functions should play in responding.

Based on a review of the EU AI Act, Gartner has identified several key activities organizations impacted by the Act should take, as well as common owners of, and partners involved in, those actions. Our recommendations cover both direct requirements of the Act as well as activities designed to strengthen the organization's overall governance of AI risk. This checklist can be used as a starting point for achieving compliance and providing ongoing risk management for AI. To eliminate gaps, minimize overlap in risk management, and facilitate clear understanding of roles, responsibilities and decision rights, assurance leaders should use an assurance map to account for new responsibilities across various functions. Organizations can either build an assurance map specifically for AI governance and risk management or update existing assurance maps to cover this new risk area.

The activities required for compliance fall into four buckets:

- Governance and oversight
- Risk assessment
- Ongoing risk mitigation, monitoring, and auditing
- Policies, procedures and training

Governance and Oversight

The EU AI Act establishes a category of banned AI uses and outlines several high-risk uses. As a result, board and senior leadership must:

- Be fully informed of the Act's enhanced compliance obligations
- Provide enhanced oversight to ensure banned AI use cases are not deployed and that the organization's use of AI meets the Act's enhanced standards for transparency, fairness, security and privacy.

Table 1 details key action items regarding governance and oversight and provides a starting point for assurance mapping by identifying suggested owners and partners.

Table 1: Action Items for Governance and Oversight Following EU AI Act

Action Item	Common Owner(s)	Business or Functional Partner(s)
Embed the Act into relevant risk management and reporting frameworks (legal, enterprise, privacy, security, etc.). Assign roles and responsibilities for approving/halting use cases, and escalation criteria to adjudicate disagreements about use cases.	AI Governance Committee (see Note 1)	Business Unit Managers
Modify policies to include examples of prohibited use cases, inform business partners which use cases the EU considers high risk, codify what high-risk cases are and outline new obligations attendant to them.	Legal or Compliance	AI Governance Committee
Organize periodic strategy reviews with the Board of Directors (e.g., Full Board, Strategy Committee, Risk Committee, Audit Committee) to assess the impact of the EU AI Act on strategic initiatives or products. Determine which Board committee will have oversight of governance.	Legal and Board of Directors	Compliance, ERM, Privacy, IT Security and Data and Analytics (D&A)
Perform a strategic gap analysis to manage strategic, technical, regulatory and operational risks of AI use cases and AI systems in use in the organization and identify which are "high-risk" or "prohibited" as defined by the Act. The strategy should articulate when and how the enterprise will use AI and define the purpose of AI use cases.	AI Governance Committee	ERM

Action Item	Common Owner(s)	Business or Functional Partner(s)
Determine whether transparency, explainability, privacy and security standards and objectives for AI models are addressed by enterprisewide policy and aligned with the risk appetite.	Audit	Privacy and D&A
Determine that management has incorporated AI model fairness objectives and standards during AI systems development.	Audit	Compliance and ERM
Share Board-level training materials on AI technology and systems that address its potential benefits and limitations, as well as the risks it may pose.	Legal	IT, Security, D&A and Privacy
Establish an internal governance charter that includes standards for risk assessments and risk rankings, data usage, model ops, continuous monitoring throughout the life cycle, and security.	ERM	D&A, Engineering, IT Architecture, Privacy, IT Security
Ensure committee(s) and/or function(s) responsible for AI governance are trained on the requirements of the Act and incorporate them into risk management for AI systems (see Note 2).	D&A, Privacy	ERM, Compliance, IT Security

Source: Gartner

Risk Assessment

The Act establishes categories for high-risk uses and establishes new risk assessment requirements for companies adopting high-risk uses and providers of AI systems. [4,5] These include requirements for:

- Identifying and tracking high-risk uses of AI in the organization
- Assessing conformity of controls with the Act's standards on all high-risk AI use cases.
- Conducting a Fundamental Rights and Algorithms Impact Assessment (FRAIA) to ensure the system does not impinge on EU citizens' rights of privacy, nondiscrimination and human dignity. The European AI Alliance provides an example framework for a FRAIA. [5,6,7]

Because the EU AI Act builds on GDPR principles, many of the new requirements of the Act can be incorporated into existing risk assessment workflows. Table 2 details key action items regarding risk assessment and related activities and provides a starting point for assurance mapping by identifying suggested owners and partners.

Table 2: Action Items for AI EU Act Risk Assessment

Action Item	Common Owner(s)	Business or Functional Partner(s)
Conduct a gap assessment of your existing risk frameworks to assess how the Act impacts your risk profile, which risks are not reflected, and which interdependencies may exist.	ERM, Compliance	Business Process Owner(s)
Coordinate with IT and D&A to develop a use-case inventory tied back to "critical dependencies" such as applications or processes. You can do this by either adapting pre-existing resources, such as a model inventory, data inventory or application inventory, or using information from those resources to create a separate use case inventory.	Privacy, Compliance and ERM	Data and Analytics, IT and Relevant Business Units
Update the audit universe to incorporate existing and emerging AI systems in the organization and/or business units that own development, operations or other aspects of AI implementation. Where ownership of AI-related risks belongs with existing auditable entities, ensure that new responsibilities for AI systems are included in audit risk assessments.	Audit	Compliance, ERM and IT Security

Action Item	Common Owner(s)	Business or Functional Partner(s)
Incorporate screeners into data privacy impact assessment intake processes to identify whether an individual use meets the criteria for high-risk or prohibited use cases in the Act.	Compliance, Legal or Privacy	Project leaders and business process owners
Establish or update security or privacy impact assessments to incorporate conformity assessment requirements: • Modify questionnaires to assess the quality of datasets used to train, validate and test AI systems; technical documentation and record keeping; transparency to users; level of human oversight; robustness and accuracy of the model; and cybersecurity for high-risk use cases. [6] • Private operators providing public services and operators providing high-risk systems should conduct a fundamental rights impact assessment (FRAIA). This can be incorporated within existing EU-mandated Data Privacy Impact Assessments (DPIAs) when appropriate, or stand-alone.	Privacy, Information Security or Compliance	Project leaders and business process owners
Perform and validate risk assessments of the AI model portfolio that include: evaluation of model explainability; potential for bias and bias mitigation techniques; data management frameworks and practices; and compliance with data privacy requirements.	ERM, Audit, Privacy, Compliance	D&A and product teams developing in-house AI tools
Update due diligence or vendor assessments to include questions on: • Application security • Error or anomaly detection • Inclusion of personal, sensitive or copyrighted information in training data • Controls that vendors or third parties place on output (e.g., to minimize the generation of incorrect information that may have negative societal or personal impact) • Transparency (e.g., notice of when models will be used to automate decision-making, or when users are interacting with chatbots) • Indemnification for copyright infringement	Privacy, Information Security or Compliance	Project leaders and business process owners

Source: Gartner

Conclusion

The EU AI Act introduces additional complexity into your assurance efforts. Assurance leaders must understand the role that each function plays, and modify their governance, oversight, risk management, policies and procedures to achieve compliance.

Evidence

[1] Artificial Intelligence Act: Deal on Comprehensive Rules for Trustworthy AI, European Parliament

[2] Commission Welcomes Political Agreement on Artificial Intelligence Act, European Commission; The EU Agrees on a Path Forward for the AI Act, Gibson Dunn

[3] Artificial Intelligence — Q&As, European Parliament News

[4] The EU Act: A Primer, Center for Security and Emerging Technology

[5] Introduction to the Conformity Assessment Under the Draft EU AI Act, and How It Compares to DPIAs, Future of Privacy Forum

[6] Charter of Fundamental Rights of the European Union, European Union

[7] Artificial Intelligence, Questions and Answers, European Commission

Note 1

This refers to any committee tasked with governing AI usage, strategy or risk for the enterprise. This includes both stand-alone AI governance or steering committees, or committees with AI whose remit includes AI.

Note 2

More tech-oriented organizations should develop more comprehensive training for board members, whereas companies with less adoption/dependence can most likely incorporate the necessary information into board reporting materials.

Actionable, objective insight

Position your organization for success. Explore these additional complimentary resources and tools:

Webinar

Join a Virtual Event

Hear the latest insights from Gartner legal, risk and compliance experts at an upcoming or recorded event.

Watch Now

Report

Top Emerging Risk Trends

Explore the top emerging risk trends to monitor and mitigate.

Download Now

Research

Boost Legal Productivity With Generative AI

Discover key use cases for GenAI in your legal department.

Download Now

How We Help

Gartner for Legal, Risk & Compliance Leaders

Discover how we can help you tackle your mission-critical priorities.

Learn More

Already a client?
Get access to even more resources in your client portal. Log In

Gartner®

Connect With Us

Get actionable, objective insight to deliver on your mission-critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Learn more about Gartner for Legal, Risk & Compliance
gartner.com/en/legal-compliance/products/gartner-for-legal

Stay connected to the latest insights

Gartner®