ISACA

Understanding the EU AI Act: Requirements and Next Steps

Emerging Technology

© 2024 ISACA. All rights reserved.

CONTENTS

4 Introduction

4 Key Obligations of the EU AI Act

5 / Definitions and Scope

6 / Exceptions to the AI Act

6 / Prohibited Systems

7 / High-Risk AI Systems

7 / Risk Management

8 / Quality Management System

9 / Data and Data Governance

9 / Accuracy, Robustness, and Cybersecurity

10 / Technical Documentation, Recordkeeping, and Transparency

10 / Postmarket Monitoring

11 / Conformity Assessments

11 / Human Oversight

11 / AI Literacy

12 / Registration

12 / Reporting Serious Incidents

12 / Requirements for Deployers of High-Risk Systems

14 / Transparency Requirements

14 / General-Purpose AI Models

15 / Innovation Consideration

15 / Penalties

15 Next Steps for Practitioners

15 / Timeline

16 / Privacy Input

17 / AI Inventory and Third-Party Management

17 / Document AI System Acquisition and Use Processes

18 Conclusion

19 Acknowledgments

© 2024 ISACA. All Rights Reserved.

ABSTRACT

The rapid growth in the use of artificial intelligence (AI) technologies, especially generative AI (genAI), is driven by the myriad benefits these technologies are purported to provide. But in the interest of maximizing efficiency, some enterprises have rushed to adopt AI without considering its risk and the harms it could cause. The EU AI Act puts requirements in place for certain AI systems used in the European Union and bans certain AI uses. This white paper explores the AI Act's scope and risk categorization method, in addition to providing a high-level overview of the requirements stipulated in the regulation. It also contains next steps for practitioners looking to be compliant with the Act.

© 2024 ISACA. All Rights Reserved.

Introduction

The adoption of AI technologies has skyrocketed in the last few years. In 2019, 58% of organizations used AI for at least one business function; by 2024, that number jumped to 72%.[1] The use of genAI nearly doubled from 2023 to 2024, going from just 33% to 65%.[2]

While the adoption of AI can help enterprises operate more efficiently, there is significant risk associated with it. Numerous lawsuits have been brought against genAI companies due to alleged copyright violations.[3] Faulty AI or AI misuse can result in safety concerns, e.g., self-driving cars that have been tampered with, resulting in injury or death. AI systems trained on biased data could produce biased outcomes. Liability around AI remains murky, and it is often unclear who is ultimately accountable for harm caused by AI outputs.

The EU AI Act, which was approved by the European Parliament on 13 March 2024 and by the EU Council on 21 May 2024, could help mitigate some of the risk associated with AI, allowing enterprises to use AI technologies in a safe, ethical, and responsible way and instilling confidence in AI systems. The Act is touted as the first comprehensive AI law in the world.[4] Given the broad and thorough nature of the Act, it is possible that future AI laws and regulations could be modeled off the EU AI Act, similar to what happened with the EU's General Data Protection Regulation (GDPR).

The EU AI Act, which was approved by the European Parliament on 13 March 2024 and by the EU Council on 21 May 2024, could help mitigate some of the risk associated with AI, allowing enterprises to use AI technologies in a safe, ethical, and responsible way and instilling confidence in AI systems.

While not every enterprise around the world will need to be compliant with the EU AI Act, it is worthwhile to know the key requirements of the Act. The risk classification outlined in the Act can help enterprises think about the AI products they use and understand the risk associated with them.

Key Obligations of the EU AI Act

The EU AI Act has many layers of compliance requirements, including at the AI use case, model, system, project, and enterprise levels. These requirements may vary depending on whether the enterprise is a provider, deployer, importer, or distributor and whether the AI is high-risk, limited-risk, a general-purpose AI model, or some combination. The following is a high-level overview of some of the key requirements of the EU AI Act.

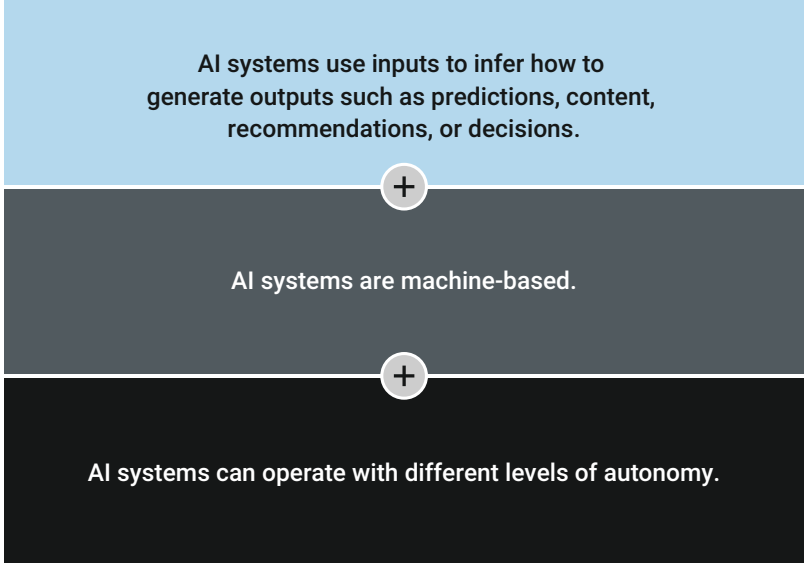
1 McKinsey & Company, "*The State of AI in Early 2024: Gen AI Adoption Spikes and Starts to Generate Value*," 30 May 2024, https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai
2 McKinsey, "*State of AI in Early 2024*"
3 Lutkevich, B.; "*AI Lawsuits Explained: Who's Getting Sued?*," TechTarget, 25 June 2024, https://www.techtarget.com/whatis/feature/AI-lawsuits-explained-Whos-getting-sued
4 European Parliament, "*EU AI Act: First Regulation on Artificial Intelligence*," 8 June 2023, https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence#:~:text=The%20use%20of%20artificial%20intelligence,world's%20first%20comprehensive%20AI%20law.

© 2024 ISACA. All Rights Reserved.

Definitions and Scope

The Act thoroughly covers what is considered an AI system. **Figure 1** shows some of the key characteristics of AI systems under the EU AI Act.[5]

FIGURE 1: Characteristics of AI Systems



The AI Act defines a risk as the combination of the probability of a harm occurring and the severity of the harm. It is crucial to understand the various roles as defined in the Act (**figure 2**).

FIGURE 2: Key Roles in EU AI Act

Providers	Natural or legal persons, public authorities, agencies, or other bodies that develop or have developed an artificial intelligence (AI) system or general-purpose AI model that is placed on the EU market. This applies to both free and paid AI systems.
Product manufacturers	Entities that manufacture products that incorporate AI systems.
Deployers	A natural or legal person, public authority, agency, or other body using an AI system, except if the system is being used for a personal, nonprofessional activity. (The majority of organizations subject to the EU AI Act will be deployers.)
Importers	A natural or legal person located or established in the European Union who places an AI system that has the name or trademark of a natural or legal person established in a third country on the market in the European Union.
Distributors	Natural or legal persons in the supply chain—other than the provider or importer—who make an AI system available in the EU market.

Note that enterprises may have a variety of roles based on the use case in question, e.g., an enterprise may be a deployer if using a third-party customer service chatbot but a provider of an AI-powered image editor. It is important to identify the applicable role based on the use case as requirements may differ for providers, deployers, and distributors.

5 Official Journal of the European Union, "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)," Article 2 and Article 3, 12 July 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401689

© 2024 ISACA. All Rights Reserved.

The AI Act stipulates requirements for AI systems that are placed on the market in the European Union. The Act defines placing AI on the market as the first availability of an AI system or a general-purpose AI model on the EU market. Making AI available on the market refers to the use of an AI system or general-purpose AI model for distribution or use in the European Union through a commercial activity, which may be paid or free. Putting AI into service refers to the first use of an AI system that is supplied directly to the deployer for use in the European Union for an intended purpose.[6]

Making AI available on the market refers to the use of an AI system or general-purpose AI model for distribution or use in the European Union through a commercial activity, which may be paid or free. Putting AI into service refers to the first use of an AI system that is supplied directly to the deployer for use in the European Union for an intended purpose.

Within the European Union, the AI Act applies to:[7]

- Providers placing AI systems on the market in the European Union
- AI system deployers that are established or located in the European Union
- AI system importers and distributors
- Product manufacturers that are putting their product and an AI system together on the market or into service in the European Union
- Authorized representatives of providers that are not established in the European Union
- Affected persons located in the European Union

Outside the European Union, the Act applies to:

- Providers placing AI systems on the market in the European Union, regardless of where the providers are located
- AI system providers and deployers outside of the European Union whose AI output is used in the European Union

Because of this wide scope, providers and deployers could be subject to the AI Act even if they are not located in the European Union. Given the extraterritorial scope of the regulation, it is crucial that all enterprises determine if the Act's requirements apply to them.

Exceptions to the AI Act

The EU AI Act does not apply to all AI systems on the market in the European Union. AI systems intended for military, defense, or national security activities are excluded, even if used by a private entity. But if those systems are, even temporarily, used for other purposes, they would be subject to the regulation.

The AI Act is also not applicable to AI systems used solely for scientific research and development, but there are requirements for AI systems or models that need to be tested in real-world conditions.[8]

Prohibited Systems

Certain AI practices that are deemed too risky are banned by the AI Act. **Figure 3** indicates these practices. Prohibited systems are those that could cause significant harm to individuals; these practices could result in privacy violations, discrimination, and limitations of individual freedom. AI systems that are used for the purposes outlined in **figure 3** may not, barring certain narrow exceptions, be placed on the market or used in the European Union.[9]

6 European Union, "*Artificial Intelligence Act*," Article 3
7 European Union, "*Artificial Intelligence Act*," Article 2
8 European Union, "*Artificial Intelligence Act*," Article 2
9 European Union, "*Artificial Intelligence Act*," Article 5

© 2024 ISACA. All Rights Reserved.

FIGURE 3: AI Practices Prohibited by the EU AI Act

Banned AI Practice
Artificial intelligence (AI) systems that subliminally or intentionally use manipulative/deceptive techniques to affect the behavior of a person or group of people by affecting their capability to make an informed decision, resulting in them making a decision that they would not have made otherwise or that may cause themselves or others significant harm
AI systems that exploit a person's or persons' vulnerabilities, e.g., due to age or disability, to distort the behavior of that individual in a way that could cause that person or someone else significant harm
AI systems that provide a social score on individuals based on their social behavior or personality that leads to detrimental or unfavorable treatment of individuals
AI systems that use profiling to predict the risk of a person to commit a crime
AI systems that scrape CCTV or the Internet to build a facial recognition database
AI systems that aim to detect a person's emotions in the workplace or in educational institutions
Biometric AI categorization systems that label people based on biometric information to determine their race, political beliefs, trade union membership, religious/philosophical beliefs, or sex life/sexual orientation
AI systems that leverage real-time biometric identification in public places for law enforcement purposes (some exceptions apply, e.g., for victims of abduction, prevention of imminent threats to life, etc.)

High-Risk AI Systems

Much of the EU AI Act focuses on the obligations for high-risk AI systems. In contrast to prohibited AI systems, high-risk AI systems may be placed on the market in the European Union, provided that several requirements are met. The obligations for high-risk systems apply to:[10]

- AI systems that are a safety component of a product
- Biometrics
- Critical infrastructure, e.g., water supply
- Education and job training, e.g., admission, cheating detectors
- Employment and employee management
- Essential public services and benefits, e.g., emergency services
- Law enforcement
- Immigration and border management
- Judicial and democratic processes

These systems are not considered high-risk in cases where the system does not pose a significant risk of harm to the health, safety, or fundamental rights of individuals, or influence the decision making of individuals.

The following are key obligations for providers of high-risk AI systems.

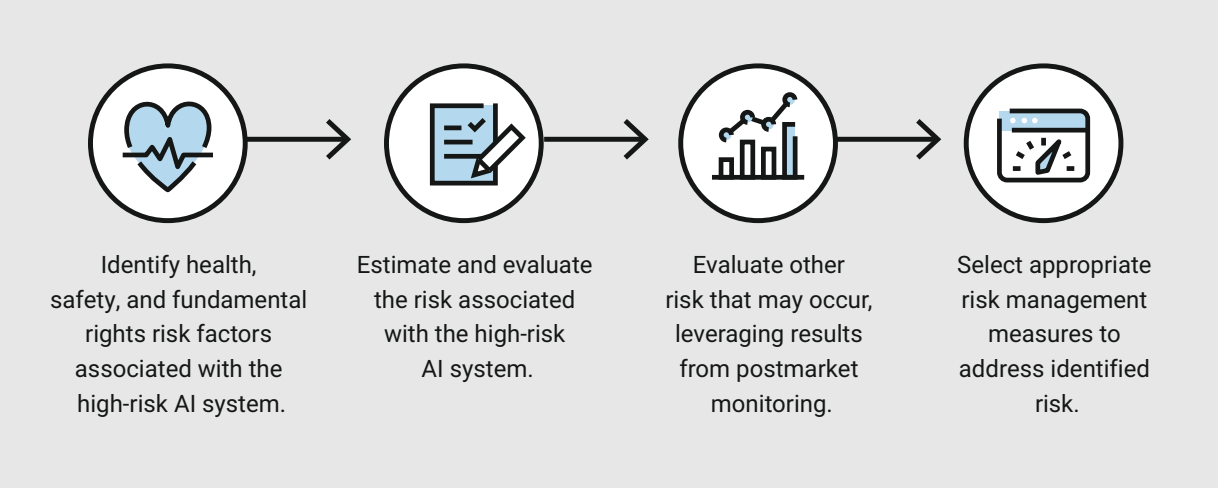
Risk Management

A risk management system is required for high-risk AI systems. The risk management process, which should span the entire life cycle of the AI system, must be iterative and updated as necessary. **Figure 4** shows the risk management steps required by the EU AI Act. The risk management system must also factor in whether any of the risk will affect people under the age of 18 or other vulnerable groups.[11]

10 European Union, "*Artificial Intelligence Act*," Article 6 and Annex III
11 European Union, "*Artificial Intelligence Act*," Article 9

© 2024 ISACA. All Rights Reserved.

FIGURE 4: Risk Management Steps



High-risk AI systems should be designed and tested to validate that they are compliant and to help determine optimal risk management measures. This should be an iterative process; because AI systems can evolve and the ways in which they are used can also change, validating compliance and reevaluating risk management measures cannot be a one-time activity.

Quality Management System

Under the AI Act, providers of high-risk AI systems must have a quality management system in place to help ensure compliance. It should be comprised of written policies, procedures, and instructions. The quality management system should account for:[12]

- Conformity assessment procedures
- Procedures for modifications to the high-risk system
- Procedures and techniques for the design, development, quality control, and quality assurance of the high-risk AI system
- Test and validation procedures throughout the development life cycle of the high-risk AI system
- Data management systems and procedures
- The risk management system
- The postmarket monitoring system
- Processes around the reporting of serious incidents
- Communication processes
- Recordkeeping systems and processes
- Resource management
- A framework outlining relevant responsibilities and corresponding accountability

12 European Union, "*Artificial Intelligence Act*," Article 17

© 2024 ISACA. All Rights Reserved.

Data and Data Governance

Given that high-quality data is a prerequisite for effective and ethical AI models, the EU AI Act has several requirements around data and data governance for high-risk AI systems. Data sets should contain accurate information, and potential bias must be identified and mitigated as well as possible. These requirements apply to training data, validation data, and testing data.[13]

Figure 5 shows the dimensions of data quality that should be considered.

FIGURE 5: Dimensions a Data Quality Plan Can Measure

Data Terminology	Measure
Accuracy	Is the data true to original intent? Is it precise?
Completeness	Are all required data attributes captured?
Coverage	Are needed data records available?
Conformity	Does the data align to required standards?
Consistency	Does the data adhere to any internally or externally mandated patterns? Is it uniform?
Duplication	Are the data records or attributes redundant?
Relational Integrity	Are data relationships (e.g., parent and child links) accurate?
Timeliness	Is the data current and available for use when needed?
Uniqueness	Is the data unique or are there duplicates?

Source: ISACA, *Applied Data Management for Privacy, Security and Digital Trust*, 2023

While it is important to maintain data quality, the EU AI Act has also stressed the need for well-defined and well-documented data collection and data preparation processing operations (e.g., annotation, labelling, cleaning, enrichment, and aggregation) covering different stages of the data life cycle.

Accuracy, Robustness, and Cybersecurity

The EU AI Act requires accuracy, robustness, and cybersecurity measures for high-risk AI systems. Technical and organizational measures for resiliency purposes must be in place. Backups, redundancy solutions, and fail-safe plans may be used to support robustness.

High-risk AI systems that continue to learn after being put into service should be designed to reduce or eliminate the risk of biased outputs that influence future operations. This may include AI systems that are open source, leverage reinforcement learning from human feedback, or use retrieval augmented generation. Mitigation measures should be in place to address feedback loops.

High-risk AI systems that continue to learn after being put into service should be designed to reduce or eliminate the risk of biased outputs that influence future operations.

Additionally, the Act requires resilience against unauthorized attempts to alter system use, outputs, or performance. There must be appropriate technical solutions in place to ensure the cybersecurity of high-risk AI systems. This should include measures to prevent, detect, respond to, resolve, and control for data poisoning, model poisoning, model evasion, and adversarial attacks.[14]

13 European Union, "*Artificial Intelligence Act*," Article 10
14 European Union, "*Artificial Intelligence Act*," Article 15

© 2024 ISACA. All Rights Reserved.

Technical Documentation, Recordkeeping, and Transparency

Demonstrating compliance for high-risk AI systems is mandatory under the EU AI Act, and it requires technical documentation for these systems *before* they are placed on the market or put into service.[15] This technical documentation can address the black-box nature of some AI systems and can help enterprises respond when AI systems do not operate as desired. The technical documentation requirements include:[16]

- A description of the AI system, e.g., its intended purpose, how it interacts with hardware and software, and instructions for use for a deployer
- A detailed explanation of the elements of the AI system and the process of its development, e.g., how the system was designed and testing and cybersecurity measures in place
- A detailed explanation of the data used in the AI system, e.g., the data requirements affecting the nature, limitations, or other factors of the data; training data sets used and their provenance, scope, and main characteristics; procedures for how the data was obtained and selected; labelling (e.g., for supervised learning); and data cleaning methodologies, including outlier detection
- An explanation of the monitoring, functioning, and control of the system
- Relevant performance metrics
- The risk management system
- Provider changes to the system through its life cycle
- A declaration of conformity
- A list of any harmonized standards applied
- A description of the postmarket monitoring plan

In addition to technical documentation, high-risk AI systems must have automatic logs over the lifetime of the system. This recordkeeping can help ensure traceability of AI systems and assist with postmarket monitoring activities. The recordkeeping must include the start and end date and time for each use, the input data and reference database against which it was checked, and the identification of people involved in the verification of the results.[17]

Technical documentation and recordkeeping ultimately facilitate transparency about how high-risk AI systems operate and the impacts of their operation. One transparency requirement in the EU AI Act is that providers must include instructions for using the high-risk AI system in a safe manner. This should include an overview of human oversight measures, any maintenance the system may require, and the anticipated lifespan of the system.

Technical documentation and recordkeeping ultimately facilitate transparency about how high-risk AI systems operate and the impacts of their operation.

Postmarket Monitoring

Given that many AI systems can evolve even after they are placed on the market, monitoring them after deployment is crucial to ensure ongoing compliance. The EU AI Act requires that providers of high-risk AI systems use a postmarket monitoring system to collect and review information relevant to the performance of the AI system so they can identify any need to immediately apply a corrective or preventative action. They must also ensure that a process is in place to report any serious incidents to relevant authorities. Postmarket monitoring should account for instances where the high-risk AI system interacts with other AI systems.[18]

15 European Union, "*Artificial Intelligence Act*," Article 11
16 European Union, "*Artificial Intelligence Act*," Annex IV
17 European Union, "*Artificial Intelligence Act*," Article 12
18 European Union, "*Artificial Intelligence Act*," Recital 155 and Article 72

© 2024 ISACA. All Rights Reserved.

Conformity Assessments

Conformity assessments show that high-risk AI systems are compliant with applicable regulations. They will assess the quality management system and technical documentation. These assessments are required for high-risk AI systems, and new assessments must occur after any substantial modification to these systems.[19]

High-risk AI systems that meet conformity assessment requirements will receive a CE marking—a physical marking for physical products, a digital one for products that are only digital. High-risk AI systems with the CE marking may be placed on the EU market.

Human Oversight

Considering the potential harm that high-risk AI systems could cause, the EU AI Act requires human oversight for these systems. The goal of human oversight is to reduce the risk to health, safety, or fundamental rights that could result from the use of high-risk AI systems. The nature of the oversight needed may vary depending on the risk, degree of system autonomy, and context in which a system is used.

Considering the potential harm that high-risk AI systems could cause, the EU AI Act requires human oversight for these systems. The goal of human oversight is to reduce the risk to health, safety, or fundamental rights that could result from the use of high-risk AI systems.

Human oversight should:[20]

- Help deployers understand the abilities and limitations of the high-risk AI system
- Bring attention to the possibility of overreliance on outputs of high-risk AI systems, especially those that provide information or decision recommendations
- Allow for the correct interpretation of the system's output
- Enable the choice to disregard, override, or reverse the system's output
- Allow for humans to intervene or stop the system's operation

AI Literacy

To maximize the value AI provides and minimize the potential harm, promoting AI literacy is essential. AI literacy refers to the knowledge and understanding required to effectively use, interact with, and critically evaluate AI systems. This includes a basic understanding of AI, technical skills, ethical and legal awareness, critical thinking, and practical application. AI literacy is crucial during all phases of the AI life cycle. The EU AI Act requires providers and deployers of AI systems (regardless of the level of risk) to ensure that anyone dealing with the operation and use of AI systems on their behalf should have a sufficient level of AI literacy.[21] AI literacy can ultimately facilitate human oversight of AI systems.

AI literacy refers to the knowledge and understanding required to effectively use, interact with, and critically evaluate AI systems.

19 European Union, "*Artificial Intelligence Act*," Article 43
20 European Union, "*Artificial Intelligence Act*," Article 14
21 European Union, "*Artificial Intelligence Act*," Article 4

© 2024 ISACA. All Rights Reserved.

Registration

Before being placed on the market or put into service, high-risk systems must be registered with the EU database for high-risk AI systems.[22] This database will contain information that is accessible and publicly available. Information for the database must be user-friendly and machine-readable.

Reporting Serious Incidents

The EU AI Act requires that high-risk AI system providers report serious incidents when they occur. The Act defines serious incidents as an AI system malfunction or incident that leads to death or harm to a person's health, serious and undoable disruption to critical infrastructure, not meeting obligations intended to protect fundamental rights, or serious harm to property or the environment.

The EU AI Act requires that high-risk AI system providers report serious incidents when they occur. The Act defines serious incidents as an AI system malfunction or incident that leads to death or harm to a person's health, serious and undoable disruption to critical infrastructure, not meeting obligations intended to protect fundamental rights, or serious harm to property or the environment.

Reports of this type are made to the market surveillance authorities of the Member State or States of the European Union where the incident happened. An incident must be reported no later than 15 days after becoming aware of it, but depending on the severity of the incident's impact, the reporting time may be less.

After the incident is reported, the provider must investigate the incident, including making a risk assessment, and apply the appropriate corrective action.[23]

Requirements for Deployers of High-Risk Systems

Enterprises deploying high-risk AI systems, models, or services have certain obligations under the EU AI Act.[24] Due diligence is crucial when selecting an AI system provider as deployers may be liable for providers' shortcomings. **Figure 6** outlines the obligations of high-risk AI system deployers.

Due diligence is crucial when selecting an AI system provider as deployers may be liable for providers' shortcomings.

22 European Union, "*Artificial Intelligence Act*," Article 49, Article 71
23 European Union, "*Artificial Intelligence Act*," Article 73
24 European Union, "*Artificial Intelligence Act*," Article 26

© 2024 ISACA. All Rights Reserved.

FIGURE 6: Obligations for Deployers of High-Risk AI Systems

Instructions for use: Deployers of high-risk AI systems must use these systems according to their applicable instructions for use.

Human oversight: High-risk systems must be overseen by people with the appropriate knowledge, training, and authority.

Data quality: Deployers that have control over input data must ensure that the input data is relevant for and representative of its designated purpose.

System monitoring: The high-risk AI system must be monitored based on the instructions for use. In the event an incident is identified, the deployer must inform the provider, importer/distributor, and applicable market surveillance authorities of the incident (in that order).

Data protection impact assessment: High-risk AI system deployers may be obligated to carry out a data protection impact assessment.

Record keeping: Automatically generated logs created by the high-risk AI system should be kept by the deployer. Note that other laws and regulations may indicate how long logs can/must be stored.

Transparency and notice: The use of high-risk AI systems, especially those used in the workplace, must be clearly communicated to impacted workers.

Cooperation: Deployers of high-risk AI systems must cooperate with applicable authorities.

© 2024 ISACA. All Rights Reserved.

Transparency Requirements

The EU AI Act includes transparency requirements for the providers and deployers of certain types of AI systems. These requirements are not specific to high-risk AI systems. Transparency about the use of AI is critical to ensuring that people trust AI, and it can affect the way in which they interact with AI. Under the EU AI Act, people interacting with AI systems must be notified that they are interacting with AI. For example, people seeking customer service support who are encouraged to talk with a chatbot must be notified that they are not speaking with a human.

Transparency about the use of AI is critical to ensuring that people trust AI, and it can affect the way in which they interact with AI.

Additionally, providers of AI systems that create synthetic content must ensure that outputs are marked as artificially generated or manipulated. Providers must consider technical limitations and capabilities of this marking, and being informed of what is considered state-of-the-art in this field is important.[25] Watermarking AI-generated or -manipulated content can help mitigate the harm spread by deepfakes and limit the proliferation of misinformation and disinformation.

There are also transparency requirements for deployers of limited-risk AI systems that have emotion recognition or biometric categorization features; these deployers must notify people affected by these systems about their operation. Note that this type of sensitive personal data may also be subject to other EU regulations, e.g., GPDR.

General-Purpose AI Models

The EU AI Act considers general-purpose AI models to be AI models that can perform a variety of distinct tasks and that display generalities. Through self-supervised, unsupervised, or reinforcement learning, these models are trained on a large quantity of data. General-purpose AI models may be refined and modified into new models. The EU AI Act imposes many obligations for providers of general-purpose AI models. They must create and maintain the models' technical documentation, including training and testing processes, and this information should be made available to AI system providers who plan to incorporate the general-purpose AI models into their AI systems. Model providers must also create a detailed summary of the content that trained the general-purpose AI model, and this information must be made publicly available.[26]

The EU AI Act also outlines additional obligations for providers of general-purpose AI models with systemic risk. General-purpose AI models with systemic risk are those that have high-impact capabilities, based on various indicators and benchmarks defined in the Act.[27] Systemic risk is defined as risk that could impact public health, safety, security, fundamental rights, or society as a whole and can be disseminated at scale across the value chain. Given that it may be easier to grasp the full capabilities of a model after it is on the market and has been used more, the threshold for what classifies as an AI model with systemic risk is not a fixed point. For this reason, providers may need to reevaluate their general-purpose AI models periodically.[28]

25 European Union, "*Artificial Intelligence Act*," Article 50
26 European Union, "*Artificial Intelligence Act*," Article 53
27 European Union, "*Artificial Intelligence Act*," Article 51
28 European Union, "*Artificial Intelligence Act*," Article 55

© 2024 ISACA. All Rights Reserved.

Providers of general-purpose AI models with systemic risk must meet all the requirements of providers of general-purpose AI models outlined previously. Those who provide general-purpose AI models with systemic risk must also evaluate the model and conduct adversarial testing to identify and mitigate systemic risk associated with it; report any serious incidents and corresponding remediation to the AI Office (a group established at the EU level); and provide sufficient cybersecurity protection for the model.

Innovation Consideration

Many AI use cases are new, and AI system capabilities are evolving rapidly. The Act recognizes that the regulations it embodies may be criticized for stifling innovation. To remedy that, the Act requires that each Member State create an AI regulatory sandbox to foster innovation and facilitate the development, testing, and validation of cutting-edge AI systems before they are placed on the market.[29]

Penalties

Consequences for noncompliance with the EU AI Act vary based on the nature of the noncompliance. Noncompliance with banned AI practices is subject to fines up to €35,000,000 or up to 7% of the company's total global annual turnover, whichever is higher. Noncompliance with other provisions of the Act is subject to fines of up to €15,000,000 or up to 3% of total global annual turnover, whichever is higher. For small to medium-sized enterprises, the fines are not as severe; they are up to the previously stated percentages or amounts, whichever is lower.

Noncompliance with banned AI practices is subject to fines up to €35,000,000 or up to 7% of the company's total global annual turnover, whichever is higher.

Enterprises must supply accurate and up-to-date information to relevant authorities as necessary. Providing inaccurate, incomplete, or misleading information is subject to a fine of up to €7,500,000 or 1% of global annual turnover, whichever is higher.

Natural or legal persons can file complaints about noncompliance with the Act to the appropriate market surveillance authority.[30]

Next Steps for Practitioners

There are numerous requirements for enterprises affected by the EU AI Act. Given the consequences of noncompliance, enterprises that must be compliant with the regulation should begin working toward compliance immediately.

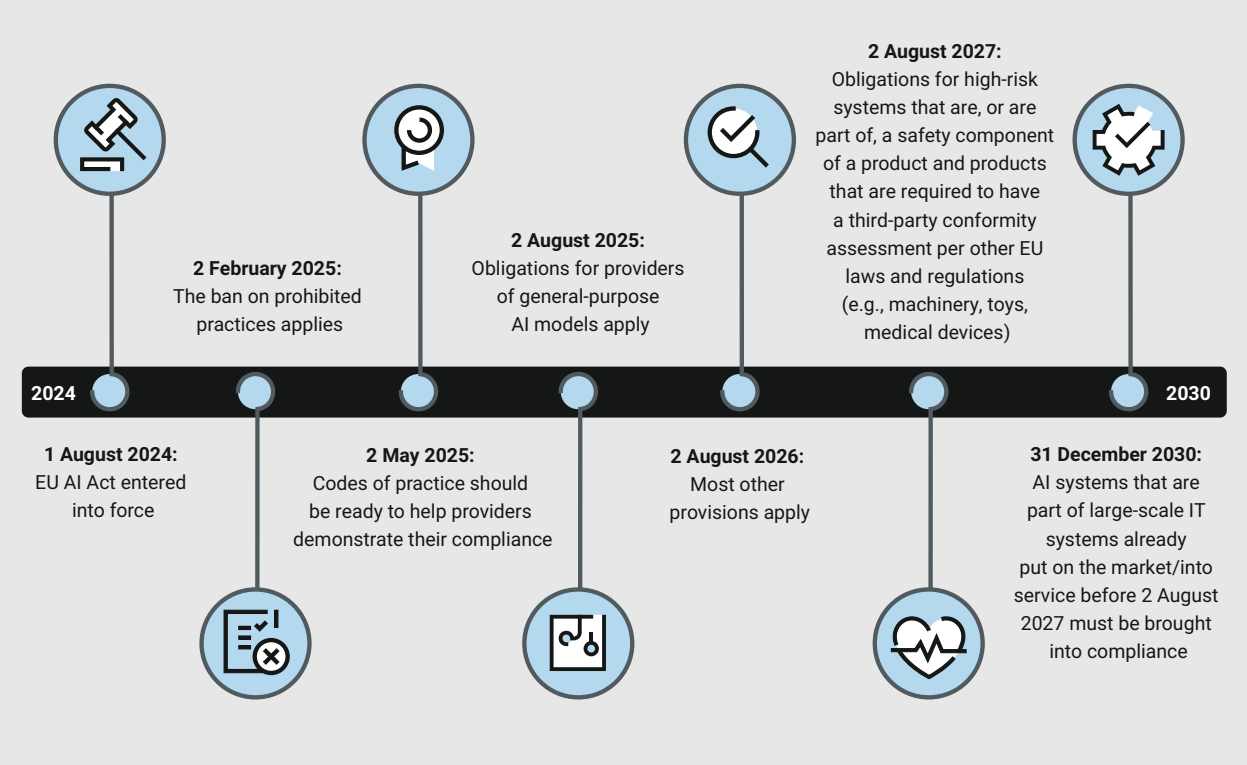
Timeline

The EU AI Act entered into force on 1 August 2024, and much of it will apply beginning 2 August 2026. **Figure 7** shows a timeline of the AI Act.[31]

29 European Union, "*Artificial Intelligence Act*," Article 57
30 European Union, "*Artificial Intelligence Act*," Article 99
31 European Union, "*Artificial Intelligence Act*," Article 113

© 2024 ISACA. All Rights Reserved.

FIGURE 7: EU AI Act Timeline



Privacy Input

Because of the many similarities between privacy regulations and AI-related regulations, an enterprise's privacy officers along with legal and compliance teams will have insight on whether the EU AI Act applies to the enterprise and how it may impact AI development and/or deployment. If it does, the team developing AI should work closely with their privacy, legal, and compliance colleagues to understand their obligations under the EU AI Act.

Many of the requirements under the Act exist today under GDPR, so enterprises will benefit heavily from taking cues from their privacy officers when it comes to areas such as risk management, data governance, recordkeeping, accuracy and robustness, human oversight and transparency. The privacy function is used to dealing with transparency, ethics, risk assessments, and accountability, where trust is key.

Moreover, AI systems require data, including personal data, which means that GDPR will apply concurrently with the EU AI Act. In addition, it is often difficult to separate personal data from nonpersonal data. This means that ensuring lawful use of the data feeding the AI model is key. In particular, there needs to be lawful grounds for using the personal data (e.g., formal consent or another type of permission granted); again, the privacy officer will be a key person involved in guiding the enterprise toward compliance with the EU AI Act. Note that collaboration with key stakeholders (e.g., procurement, risk, business, security, human resources, and technical teams) on a regular basis is essential, as enforcement actions could impact the way AI systems are used or deployed.

Legal and compliance teams can help verify that external communication requirements are met. Collaborating with user experience personnel to develop these notices can provide consumers with information about AI use that is transparent and easy to understand.

© 2024 ISACA. All Rights Reserved.

Enterprises that are not subject to the AI Act can still implement parts of it in anticipation of wider global AI-related legislation.[32] The risk-classification scheme in the Act can help enterprises classify the risk of the AI systems they use or create. Ensuring that AI systems do not cause harm can be valuable in building more trustworthy AI and is a worthwhile pursuit for all enterprises, not just those subject to the EU AI Act.

AI Inventory and Third-Party Management

To work toward compliance with the EU AI Act, practitioners need to determine the AI systems their enterprises use, create, and deploy. Identifying these systems can mitigate the risk of shadow IT.

To work toward compliance with the EU AI Act, practitioners need to determine the AI systems their enterprises use, create, and deploy. Identifying these systems can mitigate the risk of shadow IT.

Note that not all AI use will be subject to the EU AI Act or handled the same way under the Act. For example, as previously noted, an enterprise could be an AI provider in one case but a deployer in another. Regardless, enterprises should ensure that both they and any third parties they work with are compliant with the EU AI Act as appropriate. For example, if a marketing team leverages a third-party AI image generator, the enterprise would not be subject to provider requirements, but it should still ensure that the provider is compliant with the Act, for example, by verifying that AI-generated images have a watermark.

Many enterprises may have already done risk assessments of AI systems in their organization. It is important to remember that the way an enterprise has defined a high risk could differ from the EU AI Act's definition. Enterprises subject to the Act should conduct risk assessment activities that align with the Act's classification scheme.

Document AI System Acquisition and Use Processes

It is critical to have a process in place for acquisition of AI systems as well as their appropriate use. If AI is already in use, steps must be taken to ensure that it meets requirements; it is important that enterprises do not craft requirements based on existing AI systems and use cases already in place.

Service-level agreements and vendor contracts should clearly outline whether and how AI is used. In each case, AI risk must be accounted for, especially in the procurement of AI software or services. There must also be a documented process in place for how third parties will notify their customers of AI-related incidents and outages.

Enterprises, regardless of their need to comply with the EU AI Act, must establish organizationwide policies for when AI may be used, when it may not be, and situations that require escalation. To address matters that are escalated and ensure a holistic approach to AI use, enterprises should consider establishing an AI governance committee, comprised of individuals from across the enterprise who can oversee AI use in the organization.

Some key considerations for enterprises beginning an AI program include:[33]

- **Trust but verify**—Given how AI systems operate, it is quite possible that not all of their outputs will be correct. Outputs should be validated for accuracy and checked for potential bias.
- **Consider existing compliance requirements**—AI systems and models will likely use personal data, which means that applicable privacy regulations, e.g., GDPR, can apply alongside the EU AI Act.

32 This situation may be similar to what happened with the GDPR, where the European Union seemed to lead the charge for data privacy, followed by many other countries.
33 ISACA, *The Promise and Peril of the AI Revolution: Managing Risk*, 12 September 2023, https://www.isaca.org/resources/white-papers/2023/the-promise-and-peril-of-the-ai-revolution

© 2024 ISACA. All Rights Reserved.

- **Revise existing policies**—AI systems can perform a variety of tasks, but not all use cases may be compliant with applicable laws and regulations or fall within an enterprise's risk appetite. Leverage and update existing acceptable use policies or design a new one, if it does not exist.
- **Adapt existing cybersecurity and privacy policies and programs**—Promote the use of security by design and privacy by design and default in AI system development. Thinking through security and privacy considerations before partnering with a third-party AI provider can help prevent downstream cyberrisk and privacy risk and could help address compliance requirements.
- **Promote AI literacy**—Train and educate employees on AI technologies and risk. For instance, in certain cases, it may be worthwhile to provide departmental training on appropriate uses of AI specific to certain job roles, e.g., notifying a human resources department that, under the EU AI Act, they may not use AI tools to monitor employee happiness.
- **Designate an AI lead**—Someone must be tasked with tracking the AI tools in use and the enterprise's broader approach to AI. AI leads should work closely with other relevant personnel in the enterprise, including cybersecurity, privacy, legal, procurement, risk, and audit staff.
- **Perform a cost analysis**—Evaluate the cost of implementing AI systems along with any cost savings that these systems may provide.
- **Institute audits and traceability**—Given transparency and conformity assessment requirements in the EU AI Act, enterprises must ensure they understand how any AI models they create or use function. Data sources used to train AI models should be understood to help limit manipulation and mitigate against bias. Audits can provide insight into how AI systems work, helping enterprises meet transparency obligations.
- **Develop AI ethical guidelines**—Certain uses of AI may not be deemed ethical by an organization. For example, leveraging genAI to create content that customers must pay for may not be permitted. An enterprise's ethical guidelines for AI use must be documented and shared throughout the organization. Note that these guidelines may need to change as AI use evolves and as liability and copyright laws change to keep up with the evolution of AI.
- **Consider societal impacts**—The ways in which enterprises leverage AI could have significant effects on society. For example, there are understandable fears about job loss and job displacement. Deepfakes have also become quite persuasive, and people will need to be taught to identify AI-driven misinformation and disinformation. In the face of these challenges, enterprises should consider the broader social implications of their use of AI, for example by considering what the impact would be if every organization leveraged AI technology in a given manner.

Conclusion

The benefits that AI systems can provide must be balanced with the risk they pose. The EU AI Act's comprehensive risk-based approach to AI can help enterprises develop and deploy AI in a way that is safe, transparent, and trustworthy. Even enterprises not required to be compliant with the Act can implement parts of it as a best practice and in anticipation of future legislation by other jurisdictions.

The capabilities of AI systems and the laws and regulations pertaining to them are rapidly evolving, and there are unknowns with AI systems and the law, e.g., liability in the event an AI system causes a harm. Developing and using compliant and trustworthy AI is an iterative process, not a one-time activity. Staying informed about AI, how it is being used, and its potential consequences is critical to maximizing its value and limiting its harm.

© 2024 ISACA. All Rights Reserved.

Acknowledgments

Expert Reviewers

Ulrika Dellrud

AIGP, CIPM, CIPP/E, FIP, NYSB

Belgium

Carol Lee

CISM, CRISC, CDPSE, AIGP, CCISO, CCSP, CEH, CIPM, CSSLP

Hang Lung Group, Hong Kong

Board of Directors

John De Santis, Chair

Former Chairman and Chief Executive Officer, HyTrust, Inc., USA

Niel Harper, Vice-Chair

CISA, CRISC, CDPSE, CISSP, NACD.DC

Chief Information Security Officer and Data Protection Officer, Doodle, Former Chief Information Security Officer, United Nations Office for Project Services (UNOPS), Germany

Stephen Gilfus

Managing Director, Oversight Ventures LLC, Chairman, Gilfus Education Group and Founder, Blackboard Inc., USA

Gabriela Hernandez-Cardoso

NACD.DC

Former President and CEO, GE Mexico, Independent Board Member, Mexico

Jason Lau

CISA, CISM, CGEIT, CRISC, CDPSE, CIPM, CIPP/E, CIPT, CISSP, FIP, HCISPP

Chief Information Security Officer, Crypto.com, Singapore

Massimo Migliuolo

Independent Board Member, Malaysia

Jamie Norton

CISA, CISM, CGEIT, CIPM, CISSP

Partner, McGrathNicol, Australia

Maureen O'Connell

NACD.DC

Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

Erik Prusch

Chief Executive Officer, ISACA, USA

Asaf Weisberg

CISA, CISM, CGEIT, CRISC, CSX-P, CDPSE

Chief Executive Officer, introSight Ltd., Israel

Pamela Nigro

ISACA Board Chair 2022-2023

CISA, CGEIT, CRISC, CDPSE, CRMA

Vice President, Security, Medecision, USA

Tracey Dedrick

ISACA Board Chair, 2020-2021

Former Executive Vice President and Head of Enterprise Risk Management, Santander Holdings, USA

Brennan P. Baybeck

ISACA Board Chair, 2019-2020

CISA, CISM, CRISC, CISSP

Senior Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

© 2024 ISACA. All Rights Reserved.

About ISACA

ISACA® (www.isaca.org) is a global community advancing individuals and organizations in their pursuit of digital trust. For more than 50 years, ISACA has equipped individuals and enterprises with the knowledge, credentials, education, training and community to progress their careers, transform their organizations, and build a more trusted and ethical digital world. ISACA is a global professional association and learning organization that leverages the expertise of its 180,000+ members who work in digital trust fields such as information security, governance, assurance, risk, privacy and quality. It has a presence in 188 countries, including 225 chapters worldwide. Through the ISACA Foundation, ISACA supports IT education and career pathways for underresourced and underrepresented populations.

DISCLAIMER

ISACA has designed and created *Understanding the EU AI Act: Requirements and Next Steps* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

© 2024 ISACA. All rights reserved.

ISACA
1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

X: www.x.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/

© 2024 ISACA. All Rights Reserved.