2025

THE AI ACT:

ROAD TO COMPLIANCE

A Practical Guide for Internal Auditors

ECIIA

Table of **Contents**

Introduction

1. The context

In the past years, artificial intelligence (AI) has become a top priority on everyone's agenda. Public and private organisations are rapidly integrating AI systems into their processes and service offerings. In parallel there is a growing need for regulatory requirements to address the risks and concerns that come with these systems. The European Union took a significant step towards the regulation of AI with the Artificial Intelligence Act. Having entered into force in August 2024, this legislation will gradually introduce a series of requirements for all organisations that deploy, or plan to deploy, AI systems within the European market. Hence it becomes essential for organisations to prepare.

As part of their independent, objective assurance and consulting activities, internal auditors must also grasp the implications of this new piece of legislation. This paper aims to assist internal auditors in their role by providing a comprehensive overview of the AI Act and its requirements. We will start with an introduction to the AI Act. Next, we will unpack the implementation timelines and the key requirements that will be imposed on providers and deployers of AI systems.

2. The AI Act in a nutshell

The AI Act was formally proposed by the European Commission on April 2021 as a uniform legal framework for the development, deployment, and use of AI systems throughout the EU, in line with the EU's values.

One of the primary goals of the AI Act is to safeguard fundamental rights and personal data while simultaneously promoting innovation and fostering trust in AI technologies. On May 2024 the AI Act was formally adopted by the European Commission and it entered into force on August 1, 2024. The AI Act maintains significant focus around ethical considerations and the protection of fundamental rights. To that end, internal auditors should evaluate whether AI systems are developed and used in a non-discriminatory manner, promote equality, and encourage cultural diversity.

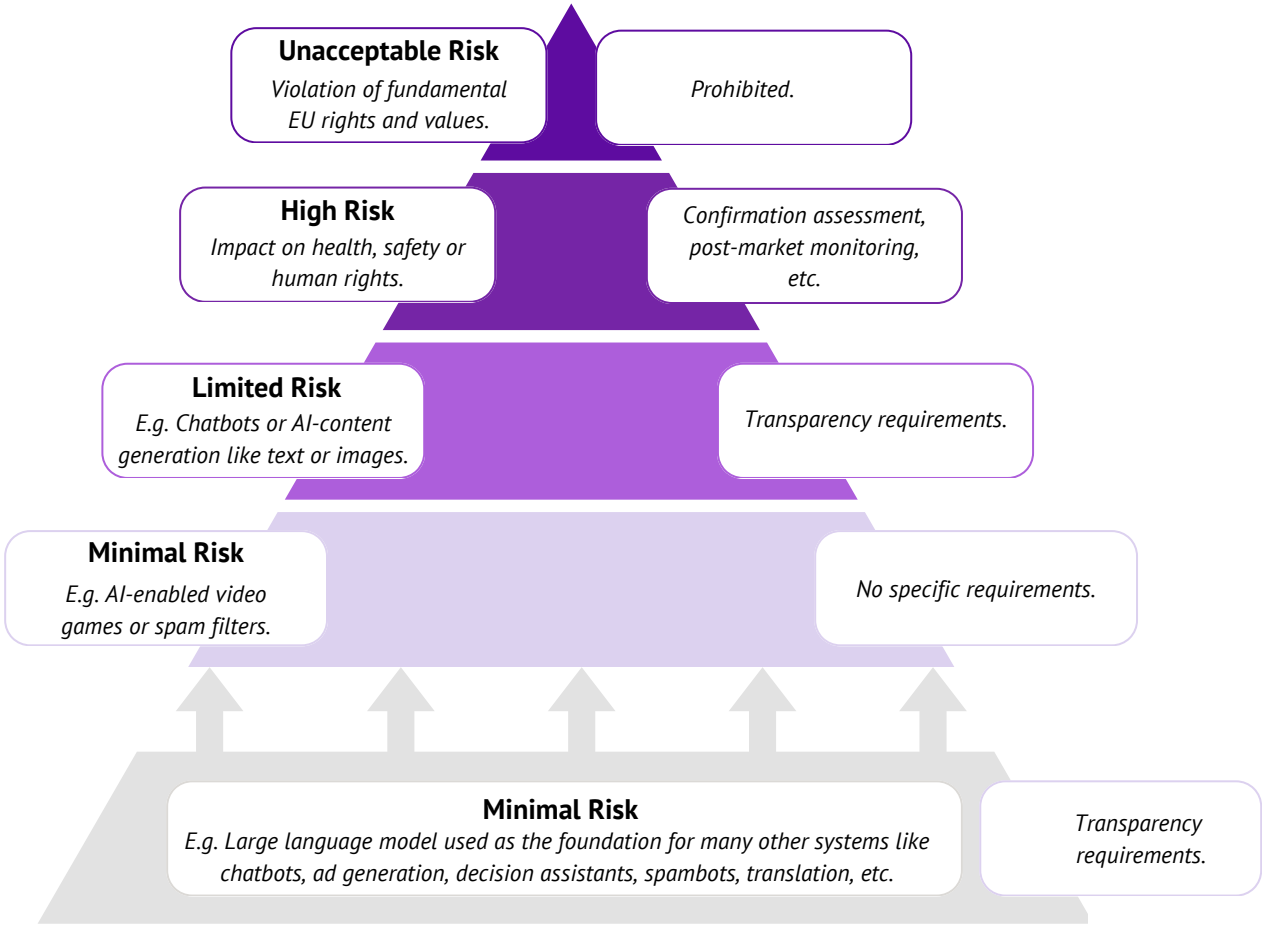
The AI Act defines AI as follows:

> *a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.*

Delving deeper into the definition, a few key characteristics stand out. First there should be some level of autonomy, indicating that systems are only considered AI when they are not based on rules solely defined by developers. It generates output from the input it receives. In addition, AI systems have the capability to infer, which means that their output can influence its environment. While providing guidance with the definition, the definition is still reasonably broad to ensure flexibility towards future AI developments that are not yet foreseen. Internal auditors should therefore challenge organisations on how they interpret the definition of AI and how they manage consistency across business units.

3. The AI Act and the risk-based approach

The regulation adopts a risk-based approach, categorising AI systems into different levels of risk:

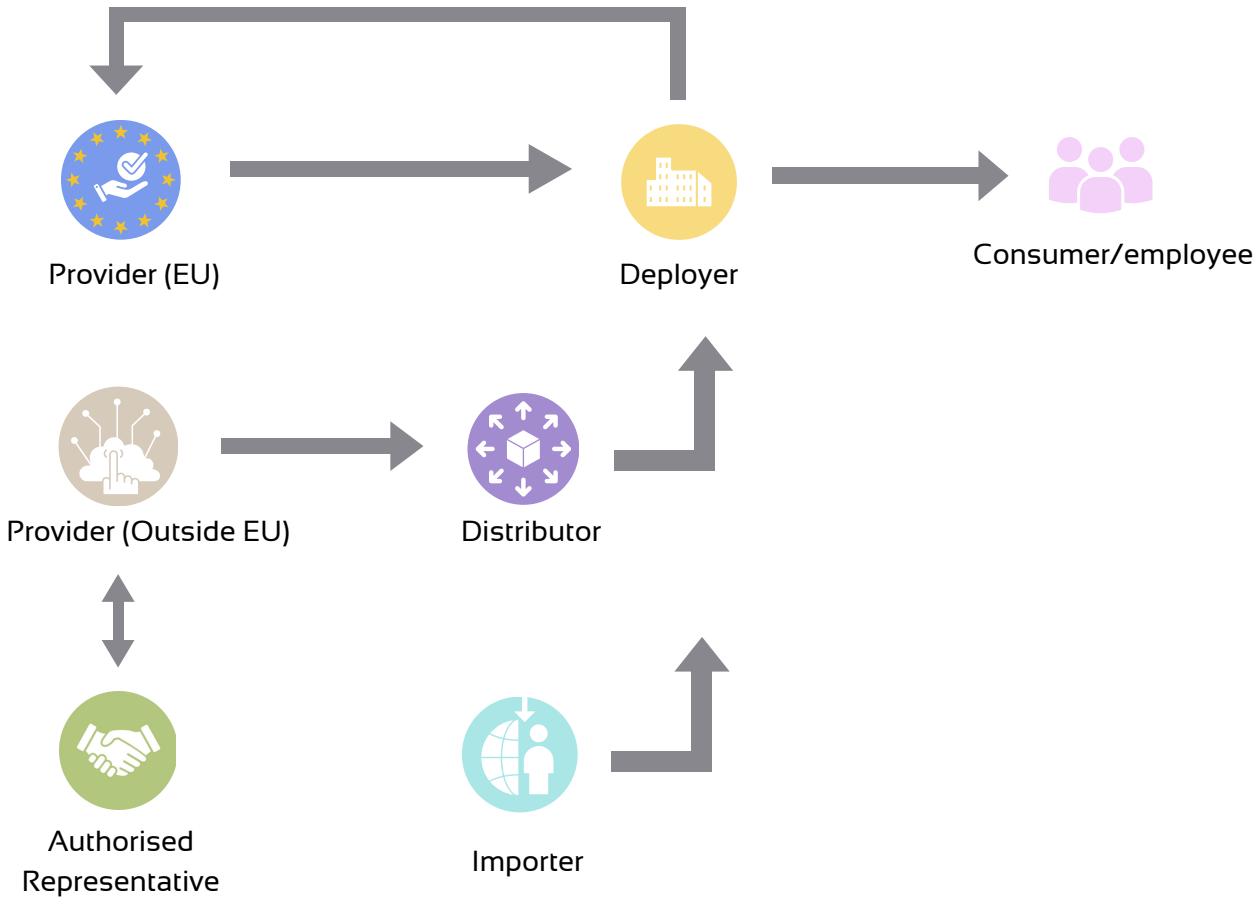


As displayed above, obligations and requirements increase based on the level of risk the AI system poses. They vary from no requirements for minimal risk AI systems, to a ban on unacceptable risk AI systems. Auditors should note that the AI Act sets clear guidelines for classifying AI systems according to these risk categories. Hence these categories can be seen as a legal definition instead of a traditional risk analysis.

In addition to the unacceptable, high, limited, and minimal risk categories, the AI Act also introduces an additional category for General Purpose AI systems (GPAI). An AI model is classified as a GPAI model when it is trained with a large amount of data and when it is capable to perform a wide range of tasks, allowing it to act as a foundational model for many other AI systems. Requirements for GPAI models increase when they are considered to have systemic risk. Again, the AI Act sets clear criteria for this increased risk category. A GPAI model is considered a systemic risk when the amount of computing used for its training is greater than 10^{25} FLOPs or if the Commission decides the model has equivalent capabilities or impact.

4. The different roles and requirements

In addition to the risk category of the AI system, requirements also vary depending on the role of the organisation in the AI value chain. The AI Act recognises several roles:



The provider and deployer are the two main roles recognised by the AI Act. The provider is the natural person or organisation (typically an AI software or hardware company) that develops an AI system or general purpose AI model and puts it on the EU market. They are responsible for compliance with the most extensive requirements set by the AI Act. When the provider is located outside of the EU, they can use an importer or distributor to put the AI model on the EU market.

The deployer is the organisation using the AI system, for example by providing it to its employees to optimise their operations or making it available for its customers. There are fewer obligations for deployers, they are responsible for ensuring proper use and adherence to the provider's guidelines. Finally, the authorised representative is a person within the EU, mandated by the provider to act on their behalf. They serve as an intermediary between AI providers outside the EU on the one hand and European authorities and consumers on the other hand.

Internal auditors should be aware that the role of their company may vary for each AI system they have. They should also note that these roles can change in time.

A deployer can become a provider when they make significant changes to the AI system or if they put it on the market under their own trademark. With such a change of roles, the company's compliance requirements also change.

A roadmap to compliance with the AI Act

1. The implementation timeline

1 August 2024

AI act enters into force.

2 February 2025

Regulations on prohibited AI systems begin to apply.

2 August 2025

Entry into force of regulations pertaining to GPAI models and public governance/enforcement of the act.

2 August 2026

All remaining parts of the AI act except Article 6(1) begin to apply.

2 August 2027

Article 6(1) begins to apply, governing the classification of products with AI safety components as high risk.

Providers of GPAI models from before August 2025 need to be compliant with the AI Act.

2. The obligations and requirements

Internal auditors must ensure that the specificities of the AI process and most specifically the requirements of the AI Act are implemented by the organisation. For high-level compliance though, Internal Auditing can regard the AI act as a compliance project like any other. They will have to evaluate the risk of AI (including the AI Act compliance), to audit AI in terms of process and in terms of governance.

Below, we outline the obligations for each of the stages in which the AI Act will come into effect and the deadlines this brings for organisations. Internal auditors can then work to ensure that their organisation is preparing for these stages in an orderly and timely manner, while adapting these high-level requirements to their particular context.

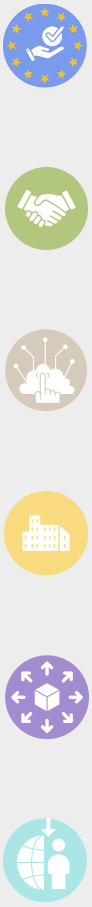
Goal	High level requirements
2 February 2025 Chapter 1 and Chapter 2	
AI literacy requirements and prohibitions on unacceptable risk AI systems start to apply.	1. A sufficient level of AI literacy of staff and other persons dealing with the operation and use of AI systems 2. An inventory of AI systems used by the company and its subsidiaries 3. A classification of the AI systems on the inventory according to the AI Act's risk categories 4. Deployers stop using AI systems with unacceptable risk 5. Providers remove AI systems with unacceptable risk from the EU market 6. Appropriate policies exist to ensure that future AI systems are evaluated appropriately
2 August 2025 Chapter III (Section 4), Chapter V, VII and Articles 78,99,100	
Appropriate measures have been taken for the deployments or provision of GPAI systems, as well as awareness of the relevant new regulatory and oversight bodies. (For preexisting GPAI systems compliance is postponed to 2027)	1. A sufficient level of institutional understanding of which public bodies the organisation will be interacting 2. Providers of GPAI systems with systemic risk notify the commission and have appropriate compliance policies in place 3. Deployers and Providers have appropriate transparency mechanisms in place

Goal	High level requirements
2 August 2026 All except Article 6(1)	
Almost all provisions of the AI act begin to apply. Appropriate policies for the previously identified AI systems are in place.	1. Risk assessment, risk management, and accountability systems for high-risk models, in place by providers and deployers 2. Transparency policies for limited risk AI systems in place by providers and deployers
2 August 2027 Article 6(1)	
Appropriate measures have been taken for the continued deployments or provision of preexisting GPAI systems and appropriate policies are in place for Chapter 6(1) relevant High risk AI systems.	1. The GPAI measures ready from 2025 are now applied to all systems. 2. Providers of products with AI components as outlined in Chapter 6(1) need to ensure their products comply with the high-risk AI obligations.

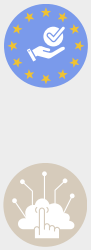
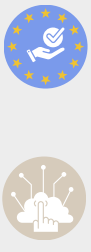
A deep dive into the obligations and requirements

As mentioned, the obligations and requirements differ depending on the risk category and the role of the organisation in the AI value chain. There are also specific requirements for General Purpose AI models. In the following overview we break down the different obligations and requirements imposed by the AI Act.

Auditors can use these insights to advise or audit the company's compliancy with the AI Act. Internal audit will need to consider the whole value chain when assessing the AI process.

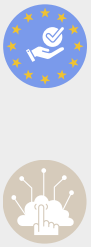
AI model type	Obligation	Roles
General obligations	**AI literacy:** measures shall be taken to ensure a sufficient level of AI literacy of those dealing with the operation and use of AI systems	
	AI registry: companies must submit their high-risk AI systems to a central AI repository. For ensuring compliancy, companies should build an AI registry, containing all AI systems they use or put on the market.	
	AI risk assessment: All AI systems on the AI registry should be risk assessed according to the risk classification method used in the AI Act. It should be noted that the classification method is prescribed within the AI act.	
Unacceptable risk AI systems AI systems considered a threat to people's safety, livelihoods, and rights. For example, using AI to: • influence people and cause significant harm, • discriminate, • profile natural persons, • create facial recognition databases, • infer emotions (except for medical or safety reasons), • real time remote biometric identification system in a public space. The precise list is found under Article 5 of the AI Act.	It is prohibited to place these AI systems on the market.	

High risk AI systems AI systems with the potential to cause significant harm: • functioning as a safety component (especially in critical infrastructure), • biometric identification and categorisation, • role in education, • decisions in employment and worker management, • law enforcement and migration, • influencing the democratic process, • making decisions for insurance, • creditworthiness or public assistance eligibility. More detail is found under Article 6 and appendix III of the AI Act.	**Risk management system** needs to be established, implemented, documented and maintained with the purpose to manage reasonably foreseeable risks throughout the entire lifecycle of the AI system.	
	Data and data governance around training, validation and testing of data sets to ensure adequate data quality, and ensure as little bias as possible.	
	Technical documentation shall be drawn up, as stated in the AI Act's appendix, before the system is put into service.	
	Record keeping of events (logs) should be in place to ensure a level of traceability of the AI system's functioning.	
	Transparency and provision of information to deployers must be in place to enable deployers to appropriately understand and use the AI's output.	
	Human oversight must be included in the design of AI systems for effective oversight by a natural person.	
	Accuracy, robustness and cybersecurity must be up to standard to ensure consistent performance of the AI system.	
	Quality management system must be in place to ensure compliance with the AI Act.	
	Documentation keeping (10 years) is required for (a.o.) technical documentation, documentation concerning the quality management system and the EU declaration of conformity.	

	Automatically generated logs must be kept for at least 6 months unless provided otherwise.	
	Corrective actions and duty information must be performed when the provider has reason to consider that the AI system is not in conformity with the AI Act.	
	Cooperation with competent authorities must be performed by providers. They must demonstrate conformity with the AI Act's requirements upon request from a competent authority.	
	Authorised Representatives must be formally appointed when they are established outside the EU and they must enable them to perform their tasks under the AI Act.	
	Conformity assessment must be performed to demonstrate compliance with the requirements of the AI Act. This can be done based on internal controls or by the assessment of the quality management system and technical documentation with the involvement of a notified body.	
	The provider shall draw up **an EU declaration of conformity** stating the AI system is in compliance with the requirements for high risk AI systems. The provider shall assume responsibility for compliance and keep the declaration of conformity up to date as appropriate.	
	CE marking of conformity must be affixed to the AI system to demonstrate conformity with the AI Act's requirements.	

	A **conformity check** must be performed when the put an AI system on de EU market for a provider located outside the EU. They must verify that the declaration of conformity and technical documentation have been drawn up and that the conformity assessment procedure has been carried out by the provider. They shall terminate their mandate if they (have reason to) consider that the provider acts contrary to its obligations from the AI Act.	 
	Registration of the high-risk AI system in the EU database, before placing on the market.	 or 
	Fundamental rights impact assessment must be performed for certain AI systems, including the intended purpose, likely risk of harm to (groups of) natural persons, a description of human oversight and other measures taken to mitigate this risk. The deployer shall notify the market surveillance authority of the result of the assessment.	
	Responsible use of AI is to be ensured by deployers. They must comply with the instructions for use from the provider. They must also assign human oversight and ensure the necessary competence, training and authority. In addition, they are responsible for the relevance & quality of input data, including the execution of data protection impact assessment and monitoring the operation of the AI system based on the instructions of use.	

	Post market monitoring must be performed by providers in a manner that is proportionate to the nature of the AI system. Based on a documented plan, it should collect, document and analyse relevant data which may be provided by deployers or other sources on the performance of the AI system throughout its lifetime.	
	Reporting of serious incidents to the market surveillance authorities is required and must be performed immediately, but not later than 15 days (of 10 days in the event of the death of a person) after the provider or deployer becomes aware of the incident.	
Limited risk AI systems The AI Act sets requirements for the limit risk AI systems, or "certain AI systems" as mentioned in article 50: • AI systems generating synthetic audio, image, video or text content • motion recognition systems or biometric categorisation systems	**Transparency obligations** are defined for providers to inform concerned natural persons that they are interacting with an AI system, unless this is obvious. Both providers and deployers of GPAI systems must provide the AI's output (e.g. images, deep fakes or texts) with a machine-readable marking to disclose that the content was artificially generated.	
Minimal risk AI systems	No requirements.	
General Purpose AI models	**Transparency obligations** are defined for providers to inform concerned natural persons that they are interacting with an AI system, unless this is obvious. Both providers and deployers of GPAI systems must provide the AI's output (e.g. images, deep fakes or texts) with a machine-readable marking to disclose that the content was artificially generated.	

	Classification of GPAI models with systemic risk must be performed by the provider. They must notify the Commission within two weeks after the requirements noted in art. 42a of the AI Act are met. Alongside they may present sufficiently substantiated arguments why the model does not present systemic risk.	
	Technical documentation of the model, its training and testing process and the results of its evaluation must be drawn up and kept up to date. They must also provide information for deployers with the capabilities and limitations of the model and publicly share a summary of the content used for training.	
	Copyright laws must be respected according to the GDPR requirements.	
	Obligations for providers of GPAI models with systemic risk also include a model evaluation, adversarial testing of the model, assessment and mitigation of possible systemic risks at Union level, reporting of serious incidents to the AI Office and ensuring an adequate level of cybersecurity protection.	

It is important to note that while not explicitly mentioned within the AI Act, AI systems are likely to be liable under other resilience EU legislation such as DORA and CSRD/CSDDD. AI systems are often supplied by third parties, have a significant upstream environmental impact, and/or present new cybersecurity and resilience issues. Many of these regulations will be also coming into effect in close proximity so it is wise for each organisation and auditing department to take the opportunity and examine the relevant AI systems not only on the requirements above but also through a wider evaluation.

A dedicated questionnaire on usage and auditing of AI system

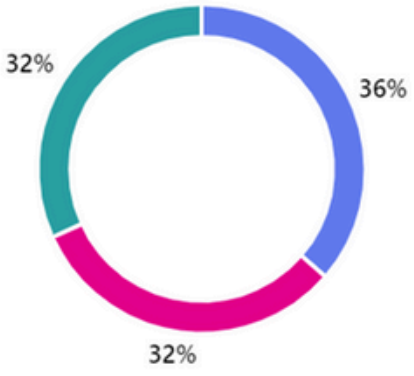
1.The survey details

To better understand the environment in which the new EU AI Act is deployed, we ran a dedicated questionnaire focused on AI Act application, AI usage and audit approach on AI.

Participant's profile

- More than 40 companies responded to the questionnaire. The profile based on the revenues, is as follows;

Less than 100 million EUR	16
Between 100 million and 1 billion EUR	14
More than 1 billion EUR	14



Among those, 39 percent are financial companies (e.g., banking, insurance) while 70 percent operate exclusively or also in Europe.

It is worth noting that in 70 percent of the cases, the respondents declared that the internal audit function counts less than 10 FTEs, while in 48 percent of the cases the same internal audit function would have no IT specialised auditor. These data, combined with an inherently disrupting technological evolution, highlight the further need to strengthen the internal audit functions, especially as regards IT skills.

2. The survey results: the AI adoption by the companies

The survey highlighted pervasive usage of AI systems, with 57 percent of the companies that either have already deployed (39 percent) or implementation ongoing (18 percent). Among these companies:

60%

A 60 percent will be subject to the new AI Act, and in most of the cases (53 percent) they have started or are going to start specific project to ensure compliance with the new regulatory requirements.

28%

Only 28 percent have defined a standard technological architecture for AI systems, while 44 percent have defined a dedicated internal regulation on AI systems development and usage.

64%

Focusing on Generative AI, 64 percent of the companies are using or are implementing Generative AI systems, while 44 percent have internal regulations on Generative AI.

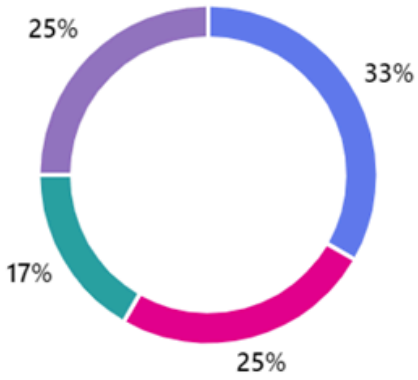
Looking at how standard AI and Generative AI systems are used, the main processes supported are:

- Customer Service, Sales and Marketing (23 percent for AI, 29 percent for GenAI)
- Business intelligence and Analytics, Finance and Accounting (27 percent for AI, 26 percent for GenAI)
- IT and Cybersecurity (11 percent for AI, 19 percent for GenAI)

3.The survey results: the internal audit function using and auditing AI

The survey highlighted that at this stage most Internal Audit departments (72 percent) are not leveraging AI systems for their activities. Anyhow, when AI Systems are used by Internal Audit, the main activity supported is risk assessment (33 percent).

Risk Assessment	4
Audit Plan definition	3
Testing activities (Test of Design or effectiveness)	2
Reporting	3



In this context, most of the respondents declared a good or fair understanding of what is meant by artificial intelligence (85 percent) and by auditing artificial intelligence systems (71 percent), While the respondents represent a technologically literate sample, they declare a low level of understanding of the AI Act (56 percent). This shows a common need to plan and deploy dedicated training activities on the new requirements introduced by the EU AI Act, ensuring the audit department are adequately skilled to provide assurance on this topic.

In most of the cases, 57 percent, Internal Audit skills for auditing AI systems are ensured through internal or external trainings, in 29 percent through knowledge sharing, and only in 14 percent through dedicated hiring.

Conclusion

The widespread and rapid technological development has seen explosive growth in the deployment of Artificial Intelligence (AI). AI is becoming an instrumental part of human society, revolutionising many aspects of life. With the many benefits AI provides, there is also a risk that the technology could produce unintended harms or be used in negative, or even unlawful ways.

To fill this void, address the rising concerns, and harness the power of AI, the European Regulator has validated the AI Act that applies to all providers, importers, distributors and deployers of AI systems that impact persons located in the EU.

The Regulators are applying increasing pressure on companies to identify the risks associated with their AI systems and manage them effectively. Therefore, it is essential that AI providers and deployers have robust risk management frameworks, comprehensive controls, and validation methodologies in place. The EU AI Act requires organisations to re-examine and, where necessary, enhance their control frameworks to meet the requirements of the Act. This will be a step towards harnessing the power of AI in a positive way, and importantly, help manage risk.

Internal auditors have an important role to play in their organisation, from advice to assurance. Without a doubt they can help them with the journey towards responsible AI and compliancy with the AI Act. So, we invite all IA shops to develop audit frameworks to assess the use of AI in their organisation and make recommendations to deliver benefits and reduce risks.

Finally, we invite the internal audit departments to lead this journey by example. Even though only few internal audit departments are using AI currently, the Act will also need to be assessed when the IA shops will use AI in their works.

Thank you!

We sincerely thank the ECIIA Working Group members for their expertise, insights, and dedication, which were instrumental in shaping this publication.

- Salvino Marigo – Head of IT&GOSP Audit, Assicurazioni Generali S.p.a.
- Luca Pellegrini – IT&GOSP Audit, Assicurazioni Generali S.p.a.
- Frank Heldens – Senior IT Auditor, Achmea
- Tomáš Pivoňka – Chief Audit and Compliance Officer, ČEZ
- Andy Watkin-Child – Founding Partner and Member, Veritas GRC
- Thaddeus Dziekanowski – Founding Partner and Member, Veritas GRC
- Pascale Vandenbussche – Secretary General, ECIIA
- Athanasios Xynogalas – Assistant Policy Advisor, ECIIA

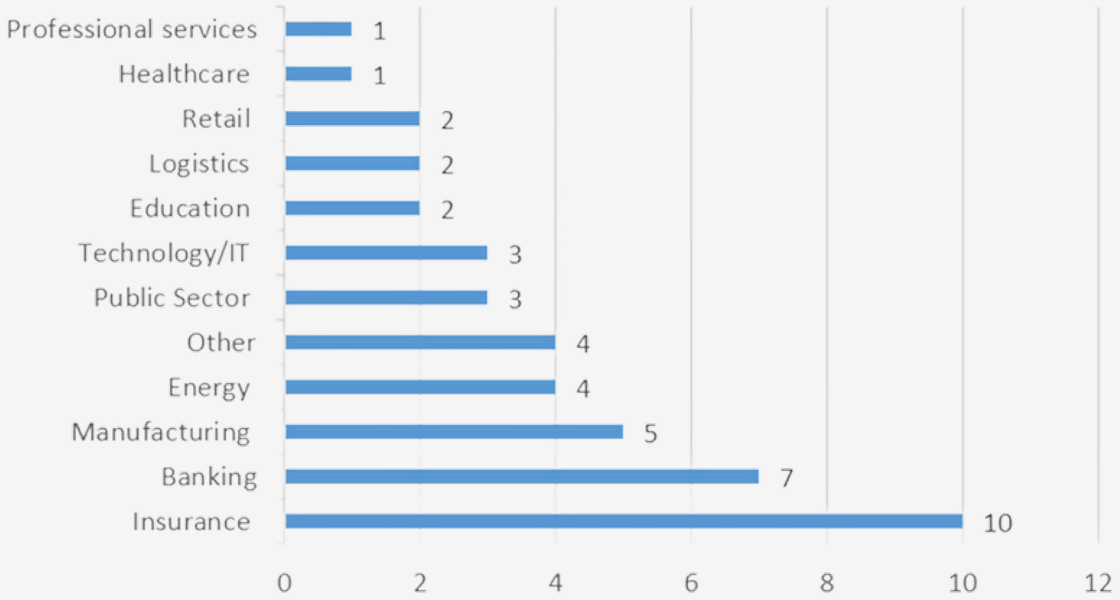
Appendix:
Survey Data

The survey has been conducted between July 2024 and October 2024. The data have been collected from internal auditors active in the private sector.

Appendix: Survey Data

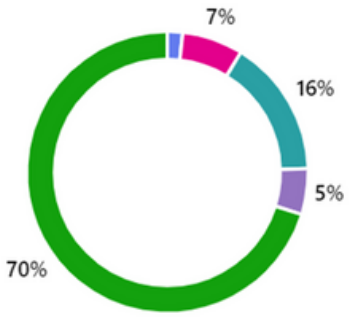
1. Population details

1. In which industry does your company primarily operate?



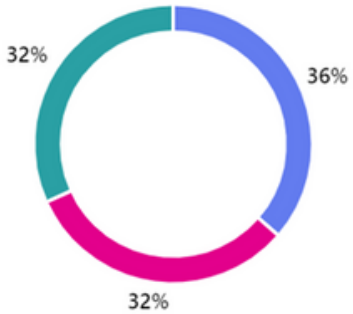
2. In which continent does your company operate?

Africa	1
America	4
Asia	9
Australia	3
Europe	40



3. What is the annual revenue of your company?

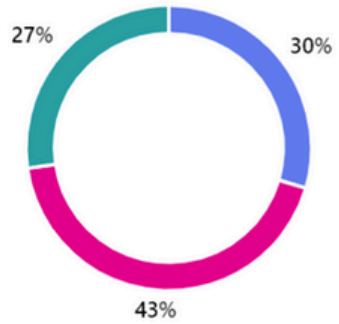
Less than 100 million EUR	16
Between 100 million and 1 billion EUR	14
More than 1 billion EUR	14



Appendix: Survey Data

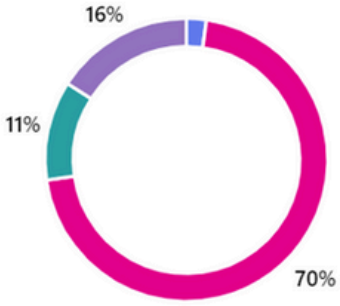
4. How many employees does your company have?

Less than 500	13
Between 500 and 10,000	19
More than 10,000	12



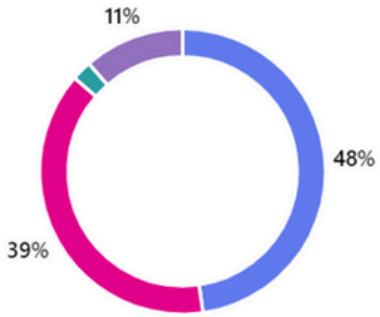
5. How many auditors are part of the Internal Audit department of your company?

None	1
Less than 10	31
Between 10 and 50	5
More than 50	7



6. How many IT (Information Technology) are part of the Internal Audit department of your company?

None	21
Less than 5	17
Between 5 and 15	1
More than 15	5

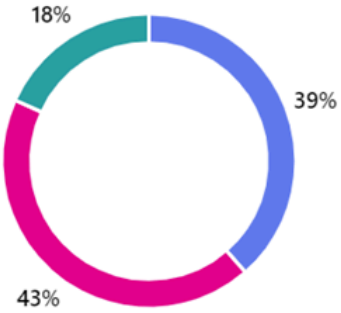


Appendix: Survey Data

2. Use of artificial intelligence - the AI act implementation status

7. Does your company use Aritificial Intelligence (AI) systems?

Yes	17
No	19
Not yet - implementation ongoing	8

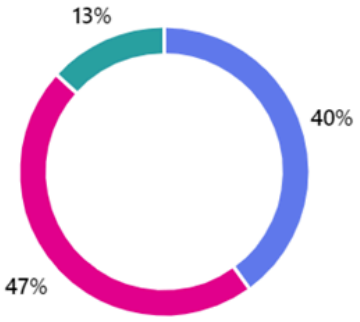


8. Is your company subject to the new EU Aritificial Intelligence Act?

Yes	15
No	10

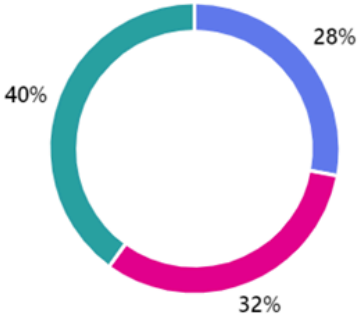
9. Has your company started a dedicated project to ensure compliance with the new AI Act?

Yes	6
Not yet, project definition in progress	7
No	2



10. Has your company defined a standard technological architecture for the implementation of AI systems?

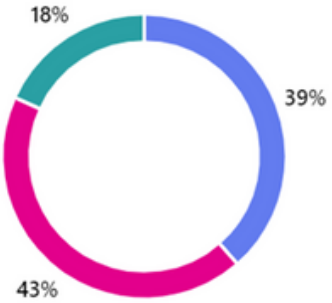
Yes	7
No	8
Don't know	10



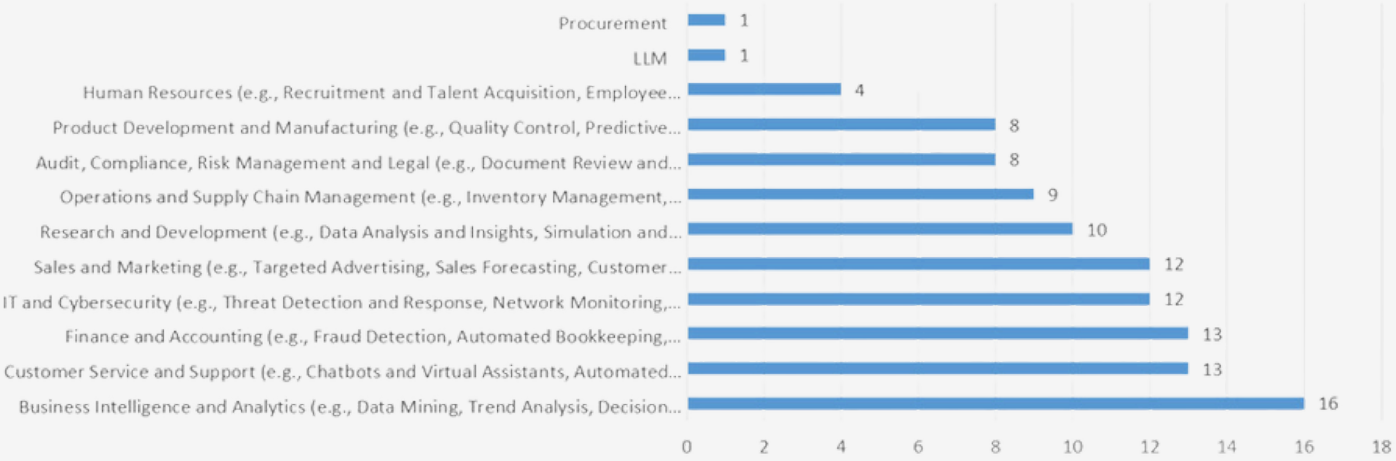
Appendix: Survey Data

11. Does your company have dedicated internal regulations in place for AI systems?

Yes	11
No	14

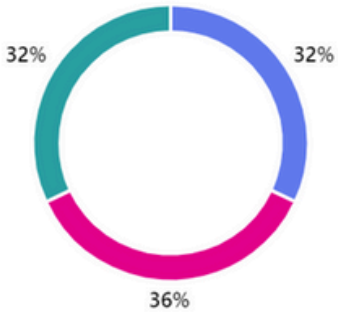


12. Which processes are supported by the usage of AI systems?



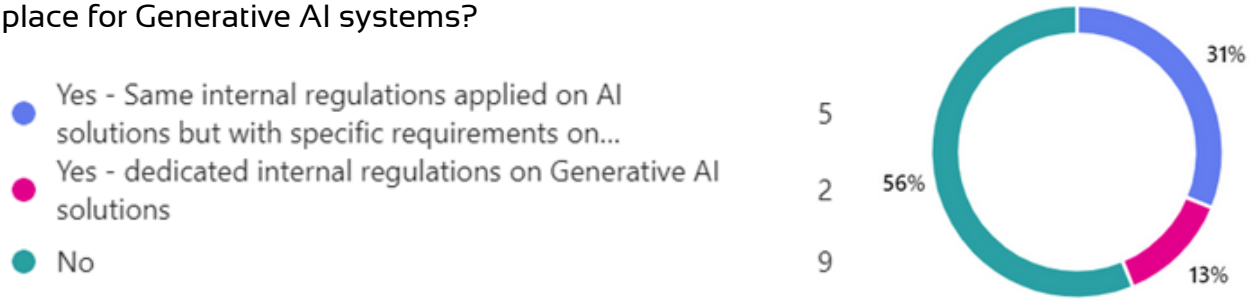
13. Does your company use Generative AI systems?

Yes	8
No	9
Not yet - implementation ongoing	8

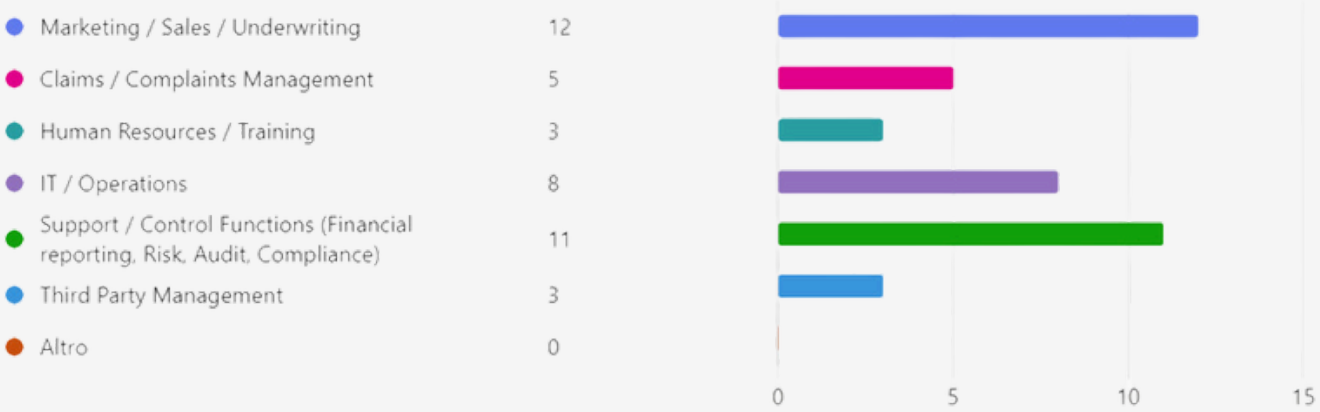


Appendix: Survey Data

14. Does your company have dedicated internal regulations in place for Generative AI systems?



15. Which processes are supported by the usage of Generative AI systems?



Appendix: Survey Data

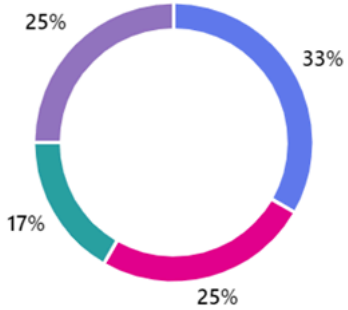
3. Internal audit and artificial intelligence

16. Does the Internal Audit department use AI systems for its activities?

Yes	7
No	18

17. Which Internal Audit activities are supported by the AI systems?

Risk Assessment	4
Audit Plan definition	3
Testing activities (Test of Design or effectiveness)	2
Reporting	3



18. Please describe briefly how AI systems support Internal Audit activities.

7 answers

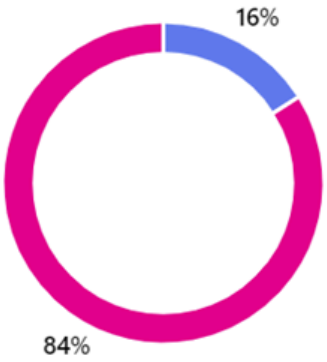
2 interviewees (29%) answered risks to this question

Appendix: Survey Data

19. How would you rate the level of knowledge within the Internal Audit department on:

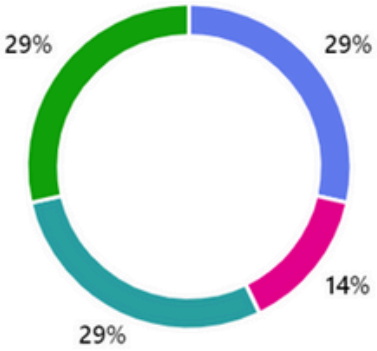
20. Does the Internal Audit department have an audit framework for auditing AI systems?

Yes	4
No	21



21. Which of the following standards are considered by the audit framework on AI systems?

ISO/IEC 23053:2022 - Framework for AI systems using Machine Learning	2
ISO/IEC 42001:2023 - AI Management system	1
ISO/IEC 23894:2023 - AI Guidance on risk management	2
NIST AI Risk Management Framework 1.0	0
Other	2



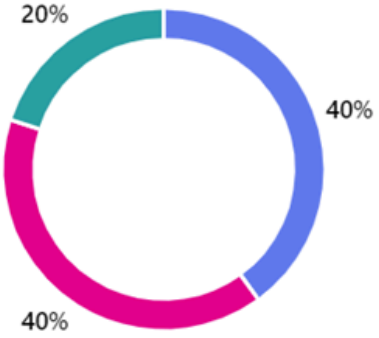
Appendix: Survey Data

22. Have audit activities been performed on AI systems?

Yes	2
No	23

23. Which approaches were used to perform on AI systems?

Internal regulations review	2
Project/Technical documentation review	2
Deep technical review - supported by specific tools	1



24. Does the Internal Audit department plan to audit AI systems?

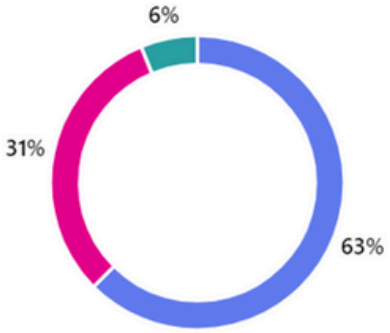
Yes	10
No	13

Appendix: Survey Data

1 interviewees (10%) answered de defined to this question

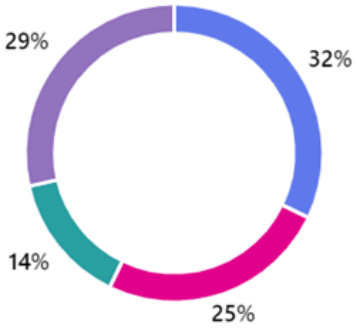
25. Which approaches will most likely be used to perform audit on AI systems?

Internal regulations revieiw	10
Project/Technical documentation review	5
Deep technical revieiw - supported by specific tools	1



26. How does your Internal Audit department ensure adequate skills for auditing AI systems?

Internal Training Programs (e.g., Specific course/webinar/conference, Regular AI Workshops,...	9
External Training programs (e.g., Enrolling in certication courses, Attending Industry conferences...	7
Hiring practices (e.g, Recruiting EI specialists, Hiring AI consultants and experts)	4
Knowledge sharing and collaboration (e.g., Internal knowledge sharing sessions, AI community of...	8
Other	0



ABOUT US

The European Confederation of Institutes of Internal Auditing (ECIIA) is the professional representative body of 34 national institutes of internal audit in the wider geographic area of Europe and the Mediterranean basin.

The mission of ECIIA is to:

- Advocate the profession of internal auditing, and promote the role and value of internal audit and strong corporate governance to European regulators and other European stakeholders;
- Support the National Institutes in advocacy activities and related services

European Confederation of
Institutes of
Internal Auditing

www.eciia.eu

Avenue des Arts 6, 1210 Brussels, Belgium

TR: 84917001473652