Empowering adequate governance for a Trusted Artificial Intelligence transformation journey

The role of Risk Management and Internal Audit

It's been more than a year since Generative Artificial Intelligence (AI) burst onto the scene, and its capabilities continue to evolve at the speed of light, making headlines daily. The increasing Generative AI landscape presents organizations with unprecedented opportunities for transformative growth, provided these advancements are adequately understood, managed, and governed. Failure to do so can result in disaster as the recent DPD chatbot fiasco demonstrated[1]. Following a system update, the AI chatbot unexpectedly started swearing at customers and criticizing DPD. The incident quickly went viral on social media, prompting DPD to disable the problematic chatbot. Undoubtedly, organizations must figure out what their governing and controlling structure around AI should be to successfully adopt it.

While Generative AI offers immense potential as a catalyst for innovation and efficiency, it also introduces inherent risks and complexities. From staff unpreparedness to data privacy concerns to operational disruptions, organizations face a wide variety of challenges associated with Generative AI adoption. Next to these internal challenges, new AI regulations are arising such as the European Union AI Act, which emerges as a pivotal regulatory development in the field of AI. This landmark legislation aims to establish a comprehensive framework for the ethical and responsible use of AI technologies. The EU AI Act outlines strict guidelines for high-risk AI applications, emphasizing transparency, accountability, and user protection. The legislation sets a precedent for global AI governance by encouraging innovation while prioritizing human-centric values. Most of the obligations outlined in the AI Act are expected to become effective by the first half of 2026.

As organizations navigate this rapidly evolving Generative AI landscape, they must contend with not only the start of regulations but also the need for their own governance and internal standards. This duality underscores the critical importance for establishing robust AI Governance frameworks to ensure ethical, transparent, and accountable AI deployment within the organization. Through having the right governance mechanisms in place, organizations can utilize AI to their fullest advantage and experience positive outcomes and competitive advantages, while mitigating risks effectively. Within this AI transformation journey, the importance of the Risk Management and Internal Audit Functions comes into play to ensure the establishment of, and assurance over, sound and effective AI governance frameworks.

In this article, we deep dive into the role and responsibilities of Risk Management and Internal Audit professionals on AI Governance. From Risk Management's involvement in the oversight of AI initiatives to Internal Audit's assurance over AI tooling, solutions, and processes, we explore how organizations can navigate the complexities of AI governance to build trust, mitigate risks, and seize opportunities.

The importance of establishing effective AI Governance Frameworks

AI governance can be defined as the set of monitoring mechanisms, policies, procedures, and controls implemented to oversee and regulate the development, deployment, and usage of AI technologies. Its significance lies in its ability to provide a structured framework for organizations to navigate the complexities of AI adoption while mitigating risks and ensuring compliance with regulatory requirements.

The EU AI Act by the European Union underscores the strategic obligation for organizations to establish proper governance frameworks around AI. Organizations must proactively adapt to these regulatory developments by implementing robust AI governance frameworks to

[1] https://www.bbc.com/news/technology-68025677

manage the associated risks effectively. Failure to establish robust and effective AI governance frameworks can lead to several significant threats for the organization. Some key risks from the lack of adequate AI Governance include:

- **A vision and strategy not adaptable to technological advancements** may result in inadequate AI implementation or lack of innovation reducing competitiveness and leading to client loss.
- **Absence or ambiguity in AI-related policies and procedures** can lead to inconsistent practices, ethical concerns, and non-compliance with regulations. In addition, the lack of clear guidance can lead to organizational sensitive data being provided to inappropriate external AI solutions.
- **Low AI literacy levels** can lead to misunderstandings, misapplications, and decision-making biases, compromising the ethical use of AI technologies.
- **Lack of transparency on (third-party) AI tooling and solutions inventory** may expose the organization to unforeseen risks, including security vulnerabilities and ethical concerns.
- **Failing to transparently communicate AI-related risks** may erode stakeholder trust and lead to increased scrutiny from regulators and the public.
- **Practices not aligned with regulatory requirements** may expose the organization to legal and reputational risks, leading to potential fines or sanctions.

By establishing clear governance frameworks for AI deployment, development and usage, organizations can maintain principles of transparency, fairness, and trustworthiness in their AI initiatives and mitigate the above-listed risks. This is particularly important given the potential societal impact of AI technologies and the need to continuously build and reinforce stakeholder trust. Effective AI governance frameworks should cover key domains which we explore later in this article. A few of these key domains are:

- **Vision & Strategy:** Creating a future-proof strategy for AI utilization and growth that aligns with business needs and regulatory landscape. It guides decision-making, secures stakeholder buy-in, and ensures AI initiatives create organizational value.
- **Governance and oversight:** Setting up a framework for decision-making and oversight, including defining the roles and responsibilities of different stakeholders involved in AI initiatives. This ensures clear accountability and transparency in the AI development and deployment process.
- **Policies and procedures:** Establishing policies and guidelines that dictate how AI should be developed, used, and maintained within the organization. These policies ensure accountability, compliance with laws and ethical standards, and alignment with organizational values and objectives.
- **AI Landscape & Inventory:** Cataloguing of AI technologies to guide decisions on resource allocation and strategic planning, understanding current and potential AI infrastructure within the organization.
- **AI Competences & Training:** Developing and managing AI skills within the organization, fostering a culture that values adaptation and learning, and ensuring staff maintain competences to responsibly utilize AI tools, upholding ethical and legal standards.

In summary, effective AI governance is critical for addressing risks associated with the deployment and development of AI technologies and ensuring compliance with regulatory requirements. In this context, the roles and responsibilities of Risk Management and Internal Audit professionals are critical and can be easily forgotten or neglected.

The responsibilities of Risk Management

In the context of AI governance, Risk Management (RM) has a crucial role as part of overseeing AI initiatives integrated within the overall business strategy. Positioned to support protecting the organization's value, Risk Management is instrumental in ensuring that AI deployment and potential in-house developments are consistent with ethical and legal principles, while promoting accountability and transparency to all stakeholders. In this context, some of the Risk Management main responsibilities are:

- **Risk identification and assessment:** RM proactively identifies and assesses risks associated with inadequate AI deployment, development, and usage. Through comprehensive risk assessments, RM identifies potential threats, such as inadequate oversight roles, insufficient knowledge and employee training, risky third-party applications, and security or privacy breaches, enabling the implementation of targeted risk mitigation strategies.
- **Adherence to ethical and legal principles:** RM ensures, in collaboration with the Compliance Function, that AI initiatives adhere to ethical standards and comply with relevant laws and regulations. By integrating ethical considerations into risk assessments and compliance frameworks, RM facilitates the alignment of AI activities with organizational values and societal expectations. This proactive approach mitigates the risk of legal penalties and reputational damage.
- **Accountability and transparency:** RM advocates for accountability and transparency throughout the AI lifecycle. By supporting the relevant Management body, such as the AI Committee, in establishing clear governance structures and frameworks, RM fosters transparency in decision-making processes and ensures that stakeholders are informed about AI initiatives' objectives, risks, and outcomes. Transparent communication about AI algorithms, data

sources, and decision-making criteria enhances stakeholders' trust and confidence in the organization's AI governance practices.

- **Collaboration with stakeholders:** RM collaborates with various stakeholders, including Management, Strategy, IT, HR, Legal, and Compliance functions, to ensure comprehensive AI governance. By fostering cross-functional partnerships, RM facilitates the exchange of insights and expertise, enabling a holistic understanding of AI-related risks and opportunities.
- **Organization-wide understanding of AI:** RM helps to improve the organization-wide understanding of AI including its potential benefits, risks, limitations, and constraints which are essential for effective AI governance. RM supports determining how AI aligns with organizational values and implements Risk Management strategies across the AI lifecycle.
- **Continuous monitoring and reporting:** RM establishes mechanisms for continuous monitoring and reporting of AI-related risks and controls, facilitating timely detection and response to emerging threats. Through ongoing risk monitoring and reporting, RM provides senior management and oversight committees with insight into the effectiveness of AI governance frameworks and the performance of risk mitigation measures enabling informed decision-making and continuous improvement in AI governance practices.

The responsibilities of Internal Audit

Building on the foundation laid down by Risk Management, Internal Audit serves as the next layer in ensuring robust governance and Risk Management practices throughout the organization's AI journey. Internal Audit provides independent and objective assurance over the effectiveness of the organization's AI governance processes and controls. The below responsibilities serve to get the basics right, while later in the AI transformation journey, Internal Audit might move on to auditing the AI integration within the organization and, once the appropriate level of maturity is achieved, auditing the organization's own AI Project development.

- **Assurance over AI governance frameworks:** Internal Audit begins by ensuring that the organization has established the foundational elements necessary for effective AI governance. This involves verifying that adequate governance mechanisms and processes, policies, and procedures overseeing AI initiatives are effectively implemented. Internal Audit evaluates the design and effectiveness of AI governance frameworks, emphasizing the importance of clear roles, responsibilities, and decision-making structures.
- **Advisor role during the AI journey:** Internal Audit can play an advisory role throughout the organization's AI journey, offering insights and guidance to stakeholders at various stages of AI adoption. This responsibility involves providing expertise and recommendations on best practices, risk management strategies, and compliance considerations related to AI initiatives.
- **Methodologies and approaches:** Internal Audit leverages various methodologies and approaches to evaluate AI-related risks and controls comprehensively. This may include conducting risk assessments to identify AI-related vulnerabilities, conducting process walkthroughs and control testing to assess the effectiveness of AI governance controls, and leveraging data analytics and machine learning techniques to detect anomalies and patterns indicative of AI-related risks. Internal Audit tailors its audit approach to the unique characteristics and complexities of the organization-wide or specific department AI initiatives.
- **Continuous auditing:** Internal Audit emphasizes the importance of continuous auditing of AI governance processes to ensure ongoing compliance and effectiveness. This involves establishing automated monitoring mechanisms to detect deviations and anomalies in AI processes and outcomes. By conducting regular audits and assessments, Internal Audit provides assurance that AI initiatives continue to operate in accordance with ethical principles, legal requirements, and organizational objectives.

How does KPMG's AI Governance Framework support Risk Management and Internal Audit?

We have developed a framework divided into 9 key domains for an effective AI Governance within organizations. This framework addresses the relevant domains covering key governance, risk management, and compliance issues to contribute to an ethical and responsible use of AI technologies. For each domain, we have defined the role of Risk Management where embedding risk management principles as part of the AI strategy is central. As well as the role of Internal Audit, which is responsible for providing assurance on the AI governance mechanisms, policies, procedures, and controls.

The different domains can be tackled separately, from an organization-wide perspective, in depth for specific department(s) or for specific AI tool(s).

Domains	The Role of Risk Management	The Role of Internal Audit
Governance & Oversight	• Support in the establishment or improvement of the organization's AI governance and oversight mechanisms as well as the definition of the different Committees' roles and responsibilities. • Establish a dedicated team and/or Committee for AI ethics and governance to continuously monitor internal AI initiatives. • Support the implementation of adequate escalation mechanisms including the ones for addressing conflicts of interest in oversight roles. • Monitor AI laws and regulatory standards developments to ensure the organization complies in time.	• Assess the effectiveness of AI oversight structure and mechanisms within the organization. • Review and assess the roles and responsibilities of key stakeholders in AI governance. • Assess the effectiveness and adequacy of the monitoring, reporting, and escalation processes for AI-related risks and opportunities. • Review existing mechanisms for identifying and addressing conflicts of interest in oversight roles.
Vision & Strategy	• Support Management in the definition of the AI vision, ambition, and strategy by incorporating risk management and ethical considerations. • Identify risk mitigation measures for AI-related initiatives or decisions deemed high-risk through the risk assessment process and incorporate them into the overall AI strategy.	• Review the organization's AI vision and strategy to assess ethical considerations. • Assess the clarity and alignment of the AI vision and ambition with organizational goals and overall strategy. • Assess the inclusion of effective risk mitigation measures into the AI strategy and initiatives. • Assess the organization's ability to adapt to a changing technological and regulatory AI landscape through benchmarking against industry best practices.
Policies & Procedures	• Assist management in establishing AI-related policies and procedures to provide guidance on the deployment, development, and usage of AI within the organization. The guidance also includes appropriate categorization of AI systems based on the risk categories outlined in the EU AI Act. • Participate in raising awareness of AI-related policies and procedures across the organization to educate various stakeholders.	• Assess the existence, clarity, adequacy and effectiveness of AI-related policies and procedures across the organization. • Review the alignment of the organization policies and procedures with regulatory requirements and industry standards. • Ensure policies related to AI are accessible and communicated to all relevant stakeholders within the organization. • Verify that adequate processes are in place to periodically update and AI-related policies and procedures.

AI Landscape & Inventory	• Conduct a comprehensive risk assessment of the organization's AI ecosystem, including technologies, processes, and stakeholders. • Develop and maintain a complete inventory of internal and external AI solutions and tools used within the organization. Through this inventory, perform a periodic risk-based evaluation of each third-party AI vendor. • Define consistent requirements for AI-vendors assessment and elements to be included in the contract with these vendors.	• Identify and assess the suitability of external AI solutions and tools purchased or utilized by the organization. • Assess the security, privacy, and compliance aspects of third-party AI solutions and tools.
AI Awareness & Literacy	• Develop effective communication strategies that ensure clear and concise information is provided to all relevant stakeholders regarding AI-related matters. • Establish feedback mechanisms that encourage stakeholders to raise any concerns or issues in relation to AI-related matters and provide appropriate channels for addressing these concerns. • Embed risk management principles in the change management approach surrounding the AI-related initiatives.	• Assess the organization's leadership commitment to AI governance and ethical AI practices. • Assess the accessibility and effectiveness of communication channels used for AI-related updates and announcements. • Ensure that transparency is maintained when communicating AI-related strategies, risks, and outcomes to stakeholders, and when disclosing material information. • Evaluate the effectiveness of existing feedback mechanisms for stakeholders to raise AI-related concerns or issues. • Assess the organization's change management approach for the deployment, development, and usage of AI.
AI Competences & Training	• Include AI ethics and compliance elements in the AI-related training provided to the organization's employees. Consider additional training for decision-makers and executives. • Provide inputs in the assessment of required AI competences for key positions within the organization.	• Assess the organization's current AI competences, including technical skills and domain expertise and identify gaps in AI competences required for successful AI initiatives. • Evaluate the effectiveness of existing training programs in building AI competences among employees. • Assess the availability and adequacy of specific training programs for decision-makers and executives on AI topics.
Data Management, Security & Privacy	• Evaluate the effectiveness of the data management framework and identify any potential risks or weaknesses in the current approach. • Monitor third-party risks associated with data protection, storage, and access to AI tools and solutions. • Ensure compliance with applicable data protection and privacy laws and regulations. • Implement security controls and measures to maintain the confidentiality, integrity, and availability of AI-related data and ensure compliance with applicable data protection and privacy regulations.	• Assess the organization's data management framework for its suitability in handling AI-related data. • Audit the effectiveness of security controls implemented for AI-related data. • Audit compliance with data protection and privacy regulations relevant to AI-related data. • Evaluate measures implemented to ensure data integrity, confidentiality, and availability within the AI tools and solutions used by the organization.

Evaluation & Monitoring	• Support Management in developing criteria for assessing AI tools and solutions performance, including benchmarks and metrics that measure the effectiveness of AI solutions against established objectives and performance expectations. • Implement monitoring mechanisms for continuous performance evaluation, including the use of real-time data analytics, to track and evaluate the performance of AI systems against established criteria. • Incorporate an assessment of the AI initiatives and developments into the annual strategic risk assessment process.	• Audit the implementation and effectiveness of monitoring mechanisms utilized to continuously evaluate the performance of AI solutions. • Review the established performance metrics and KPIs to ensure they align with organizational objectives and regulatory requirements. • Review and evaluate the effectiveness of feedback loops and continuous improvement strategies to ensure that they are achieving desired outcomes and provide recommendations for improvement.
Documentation & Record-Keeping	• Ensure that all AI-related documentation, including algorithms and solution outputs, is complete and accurate. • Develop and implement appropriate record-keeping practices for AI-related processes and decisions to ensure that all relevant information is recorded and retained.	• Audit the completeness and accuracy of documentation pertaining to AI algorithms, models, and solution outputs. • Conduct an audit of the organization's record-keeping practices related to AI processes and decision-making. • Review the organization's document management system to assess the ease of access, retrieval, and sharing of AI-related documentation.

Embedding Generative AI in your own activities for increased value creation

In this dynamic environment, Risk Management and Internal Audit professionals should also stay relevant by embracing innovative technologies and embedding Generative AI in their own processes, to enhance effectiveness and efficiency but also keep up with their stakeholders' expectations.

Risk Management professionals can leverage Generative AI-infused tooling to enhance their risk identification and assessment processes, as well as increase decision-making capabilities by accessing higher quality industry-specific information from large datasets, saving considerable time, cost, and energy compared to manual methods. AI algorithms can scan through large volumes of structured and unstructured data to identify patterns, trends, and anomalies that may indicate potential risks or opportunities. This enables risk professionals to make more informed risk assessments and strategic planning decisions, leading to better outcomes for the organization.

Furthermore, AI can play a crucial role in reducing the cost of control for repetitive monitoring activities through advanced automation. Tasks such as data validation, anomaly detection, and trend analysis can be automated using AI, freeing up resources that can be redirected towards more strategic initiatives. By automating routine tasks, Risk Management professionals can focus their efforts on addressing high-priority risks or designing proactive stimulative risk mitigation strategies ultimately enhancing the organization's resilience and competitive advantage.

Incorporating Generative AI across the different phases of the Internal Audit process represents the next phase in the digital maturity journey of Internal Audit Functions (IAFs). This can be a transformative shift, empowering IAFs to operate with increased efficiency and effectiveness.

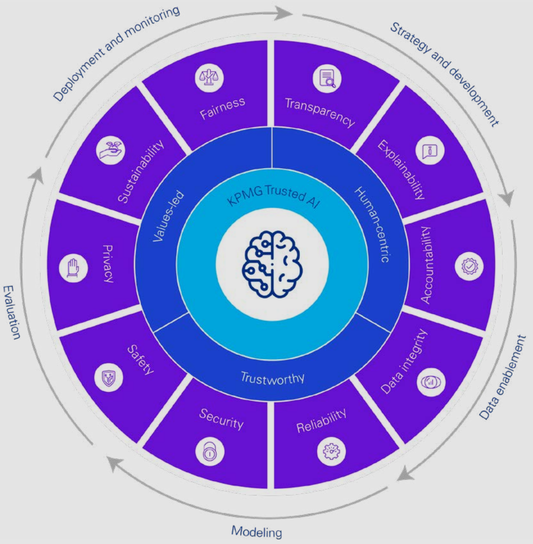
From continuously refining audit universe to streamlining data collection and audit scope definition; from enhanced analysis and audit observation generation to audit report distribution in different languages, Generative AI enables IAFs to optimize resource allocation and focus on more value-adding activities for the organization. By automating routine tasks and providing advanced analytical capabilities, AI elevates the quality and depth of audit insights, enhancing the overall value proposition of Internal Audit to stakeholders.

In summary, embedding Generative AI in both the Risk Management and the Internal Audit activities are imperative for organizations to stay relevant and effective in managing risks and conducting audits. By harnessing the power of Generative AI, risk professionals and internal auditors can unlock new levels of efficiency, effectiveness, and value creation, ensuring resilience and success in an increasingly complex and dynamic business environment.

Empowering Risk Professionals

In conclusion, effective governance and controls around AI deployment, development, and usage is not only desirable, but imperative for organizations seeking to succeed in their AI transformation journey. By implementing adequate AI governance principles and leveraging the expertise of Risk Management and Internal Audit professionals in doing so, organizations can navigate the complexities of AI implementation with confidence. Risk Management and Internal Audit professionals should recognize the criticality of AI governance in their organizations and take proactive steps to support it.

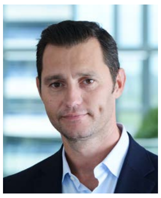
How KPMG can help



At KPMG, we stand ready to support organizations in their AI governance journey, providing guidance, insights, and tailored solutions to address their specific challenges and objectives. Our risk management and internal audit services include assessment of existing generative AI governance frameworks, benchmarking against our AI Governance framework and auditing your processes and controls. Risk Management and Internal Audit professionals should be empowered to help ensure that AI development and deployment aligns with ethical and legal principles while being accountable and transparent to stakeholders. This is where creating and operationalizing your Trusted AI framework comes in. KPMG has developed a Trusted AI framework that stresses fairness, transparency, explainability, accountability, data integrity, reliability, security, safety, privacy, and sustainability.

As organizations embark on their AI transformation journey, KPMG stands ready to be a trusted partner in their quest for responsible AI adoption. Our Trusted AI framework helps ensure that AI implementation and usage are ethical, trustworthy, and responsible. Whether it is developing AI governance frameworks, assessing AI risks, or implementing ethical AI practices, KPMG is committed to empowering organizations to harness the full potential of AI technology while mitigating risks and upholding ethical standards.

Contact

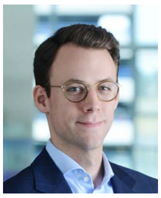


Olivier Elst
Partner
Risk & Assurance

T: +32 485 17 83 48
E: oelst@kpmg.com

Bart Van Rompaye
Principal
Head of Artificial Intelligence

T: +32 477 89 13 39
E: bvanrompaye@kpmg.com



Maxime Georges
Manager, AI and Risk
Risk & Assurance

T: +32 471 30 11 25
E: maximegeorges@kpmg.com

Thanks to Vincent Swijngedouw for his supporting contributions.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.