



Trailblazing digital frontiers

Global IT internal audit outlook

KPMG. Make the Difference.

KPMG International | kpmg.com





Contents

Foreword

03

Adapting to a dynamic risk universe

04

Can innovation fill the capability gap?

09

Technology audit maturity

15





Foreword

In today's rapidly evolving digital landscape, the role of technology audit has never been more critical. As organizations navigate unprecedented challenges and opportunities, ensuring robust IT governance, compliance and risk management is of paramount importance. A constantly shifting risk universe brings new challenges to the perspective of cybersecurity, cloud security, generative artificial intelligence (Gen AI), data privacy and blockchain, to name a few. Internal audit departments are under pressure to quickly comprehend and manage these new risks, ensure adequate coverage in the audit universe, meet reporting requirements to uphold trust with audit and governance committees, regulators, and other stakeholders while also utilizing technology effectively to maintain efficiency.

This report looks at the current, emerging and future trends impacting IT internal audit — the investment plans, delivery models and skills needed to address these trends. Our insights are augmented by key findings from KPMG International's global survey, which captures the views of over 200 chief audit executives, audit directors, vice presidents and senior managers representing internal audit teams, from a wide range of sectors across 25 different countries.

Despite an increasing number of technology audit professionals, there is an urgent need to develop skills to cope with the constant stream of new technological threats, innovate to improve audit quality, and collaborate to access essential capabilities not available in-house. And we discuss internal audit's role in enabling swift, safe and ethical adoption of Gen AI — as well as using its power to enhance audit performance.

Many organizations are currently undergoing transformations, such as the integration with ERP systems, migration to cloud computing and the adoption of AI and automation technologies. The report also explores how internal audit can add significant value, by getting involved at an earlier stage, to provide greater comfort over project and system controls. Further, internal audit teams are rapidly adopting newer operating models including

setting up of technology audit hubs that are focused on standardization and streamlining of technology audits.

We conclude with a technology audit pyramid, outlining three stages of maturity — *Foundational, Emerging and Trendsetter* — and identifying the capabilities technology internal audit teams need to reach the highest level and deliver greater value.

The survey findings and the experiences of KPMG internal audit professionals point to a pivotal role for IT internal audit in driving transformation, strengthening risk management frameworks and fostering innovation, to improve organizational resilience. I would like to thank all those who gave their valuable time to participate in this global survey. In a time of permanent disruption, I believe the insights can help internal audit teams in their quest to become even more relevant and effective.



Anil KV

Global Leader for Tech Governance
and IT Internal Audit
KPMG International and Partner
KPMG India



01 Adapting to a dynamic risk universe



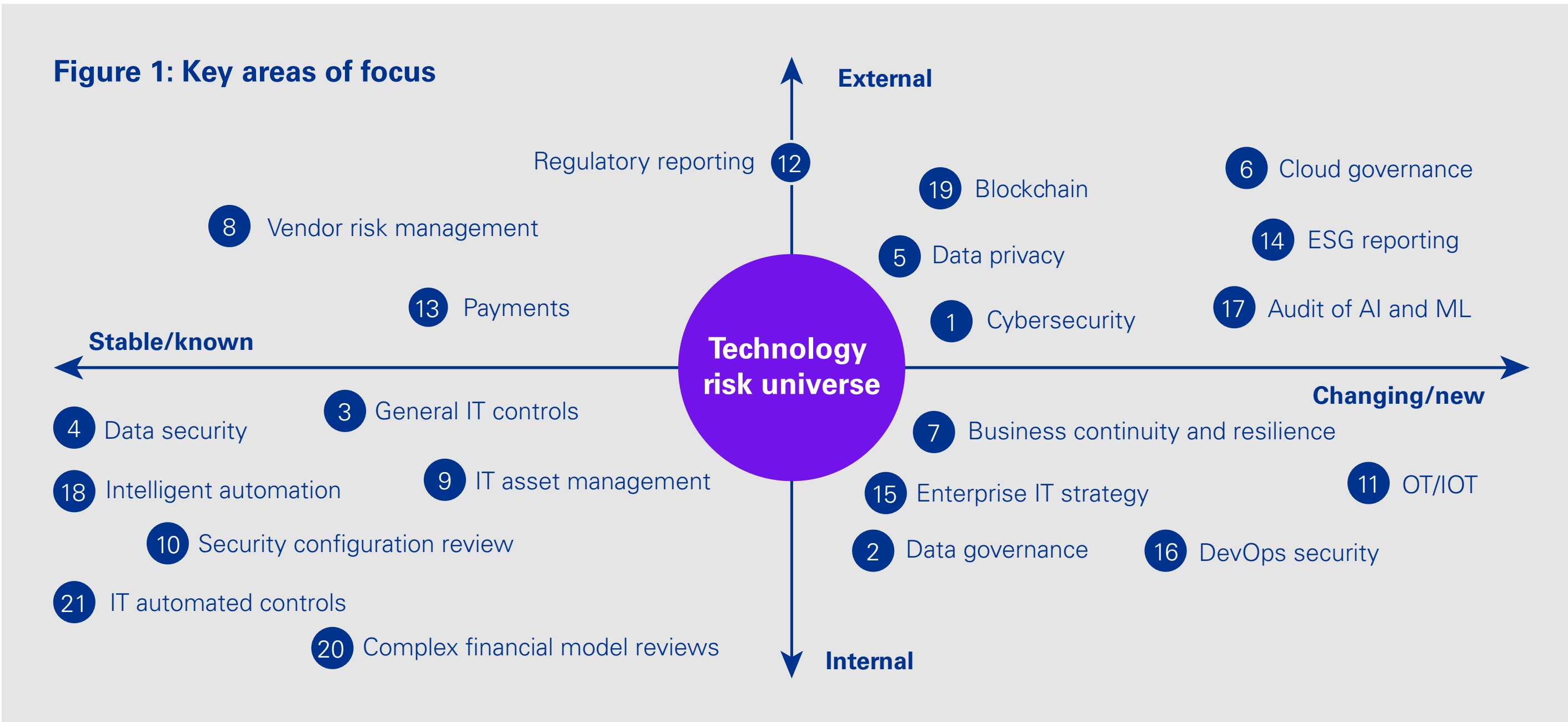
Technology risk universe

Technology risk is constantly evolving and internal audit needs to keep pace. We asked organizations to choose from the risk areas that their technology internal audit team are likely to review in the upcoming audit cycles. The areas chosen most frequently are cybersecurity, data governance and general IT controls. Based on the survey responses and KPMG professionals’ experience in advising clients on managing technology risks, key areas of focus for technology internal audit have been placed in a risk universe, portrayed in Figure 1. The horizontal axis depicts the pace of change, from static at the left to fast moving on the right. The vertical axis indicates whether the risk tends to be external (above the horizontal axis) or internal (below it).

The top three areas under scope for coming audit cycles remain unchanged since 2021 when this survey was last conducted, reflecting the immediate focus of many organizations. Information security and cybersecurity assessments, which maintain the number one spot, are a response to the rising occurrence of cyber breaches leading to loss of data and system disruption. Data underpins every activity, and data governance remains the second most important area to be audited. As Gen AI usage grows, data governance should become even more critical, and internal audit is well positioned to help identify data governance weaknesses and develop remediation plans, to avoid exposing immature data controls to threats from Gen AI.

All organizations have a technology challenge: if they don’t keep up with the latest trends, they will lose to their rivals; if they move too fast, they are vulnerable to faulty, untrustworthy data and insights, cyberattacks and loss/ theft of private data and intellectual property. Effective data governance gives employees the confidence to use AI and advanced automation to speed up operations, innovate with exciting new products and services, and generate financial and, increasingly, non-financial reports that can withstand intense scrutiny — especially in highly regulated industries. The ongoing emphasis on general IT controls as a top priority underscores the significance of traditional technology audit domains. This sustained focus reflects an understanding that, even as new areas are incorporated into the scope, the foundational assurance provided over key applications remains critical. This balanced approach ensures that while innovation is pursued, it is not at the expense of the security, integrity and availability of critical IT systems and data.

Due to the global technology transformation, new areas are becoming key focus points. Topics such as AI and ESG are being rapidly adopted worldwide, and as a result, they are becoming increasingly important in the field of evolving risks.



In this time of digital transformation and emergence of Gen AI, everything is based on data and AI is only as good as the data sets that feed into it. Data governance and AI controls are critical focus areas of IT internal audit, to confirm that organizations are meeting their customer promises and protecting themselves from ever present cyber threats.

James Buchanan
ASPAC Head of Tech Governance and
IT Internal Audit and Partner
KPMG Australia



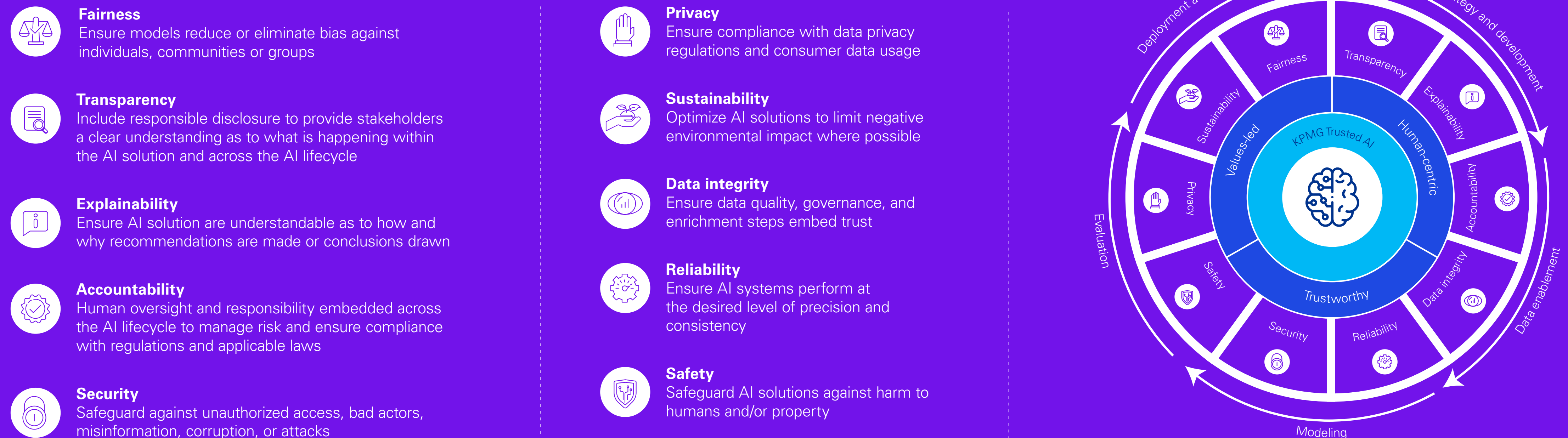
Trusted AI

Despite the rise of AI, actual audits of AI systems are still considered a relatively lower priority in terms of scope — something set to change as corporate adoption of AI increases and organizations need more assurance over new AI risks. It may be challenging to audit AI systems, readiness, governance and usage of AI tools, but internal audit can adapt and apply different techniques. Failure to do so could leave organizations vulnerable to AI risks, as well as bias from AI-driven models and algorithms fed with poor-quality data, which could lead to false conclusions.

AI is uncharted territory, and internal audit — and the rest of the organization — is still on a learning curve in understanding and alleviating the associated risks.

With its strategic approach to ethical, responsible and trustworthy AI deployment, the KPMG Trusted AI framework addresses the complexities and risks associated with AI technologies by embedding ethical standards and principles into the lifecycle of AI solutions. Its foundational principles are values driven and human-centric, using trustworthy approaches to help ensure AI is used responsibly and aligns with professional standards and values (Figure 2).

Figure 2: The Trusted AI framework



The framework emphasizes ten ethical pillars: fairness, transparency, explainability, accountability, data integrity, reliability, security, safety, privacy, and sustainability. These guide AI solutions to reduce bias, provide clarity to stakeholders, maintain data integrity, and operate reliably and securely. All of which helps build credibility and trust in the audit, reinforcing the commitment to professional excellence and public interest.

ESG Assurance

Although they face rising regulations, and a growing risk of penalties and reputational damage from poor ESG performance and inadequate disclosure, survey respondents give ESG reporting and metrics a relatively low priority. ESG may not appear to be a high risk at present, however, as organizations everywhere strive to become more sustainable and reduce their environmental impact, it is set to rise in importance and audit professionals should sharpen up their skills accordingly.

According to the survey, only one-fifth (21 percent) of IT internal audit teams are involved in ESG assessment or readiness. Data is the driving force behind ESG implementation, so auditors need to view this as a ‘technology’ issue and gain a deep knowledge of non-financial metrics and compliance, to assure the processes, controls and integrity of this data.

As ESG becomes an integral part of operations and innovation, technology is enhancing ESG auditing. A recent KPMG International article, [Tech-driven ESG: Navigating risks with precision](#), discusses internal audit’s vital role as a third line of defense, to assess ESG risks, ensure auditability of data across the value chain, and confirm that risk management is keeping pace with new regulations based upon emerging standards.



As boards place an increasing focus on ESG, organizations are increasingly generating non-financial metrics covering sustainability, supply chain integrity, working conditions, diversity and governance. IT internal audit professionals need to step up to this challenge, staying ahead of regulations, building skills, and using technologies to manage ESG risks, which include penalties for non-compliance, and potentially severe reputational damage.



Mallika Chandra
Global Program Director, IT Internal Audit
KPMG International and Director Cyber Assurance
KPMG India

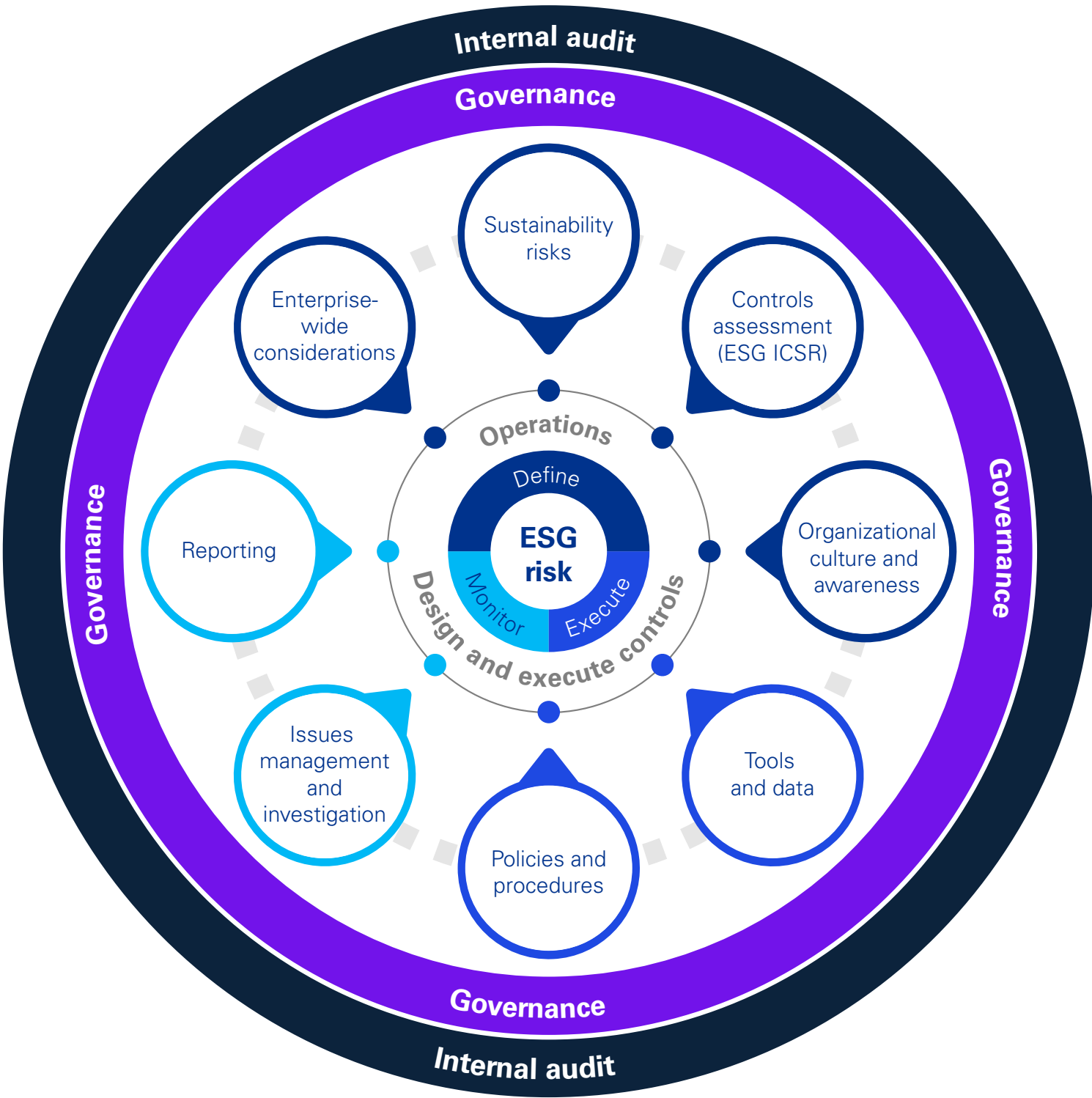


Additionally, the ‘G’ in ESG — Governance — covers cybersecurity breaches that could lower an organization’s ESG rating. As more ESG metrics go mainstream, this topic is set to rise in prominence, to help make non-financial reporting smoother and faster, and gain assurance over ESG data-gathering platforms. Different countries are moving at varied clock speeds in implementing ESG regulations, so it’s vital to regularly review developments around the world.

To address growing regulatory and stakeholder demands, digital tools are likely to dominate ESG auditing, especially the ones that integrate AI and data analytics, to conduct more accurate and comprehensive ESG reporting and compliance.

Figure 3 demonstrates some key risk domains that internal audit needs to consider while determining their ESG assurance strategy. This approach not only meets regulatory expectations but also supports strategic business goals, integrating ESG within organizational frameworks — rather than merely making superficial, unsubstantiated commitments.

Figure 3: Internal audit coverage across key ESG categories



Source: Internal Audit’s Role in ESG

Coping with external influences

Audit scope can be impacted by external factors, such as the ongoing migration of many organizations to next-generation, increasingly cloud-based or hybrid systems such as SAP S/4 HANA. However, it can be a struggle to get funding and business or IT support for such a transition.

Most successful organizations have leveraged ERP transformation by embedding internal audit and internal control streams. Our survey responses indicate that just 26 percent of internal audit teams are involved in all stages of organizational change journeys. SAP S/4 Hana

Only

26%

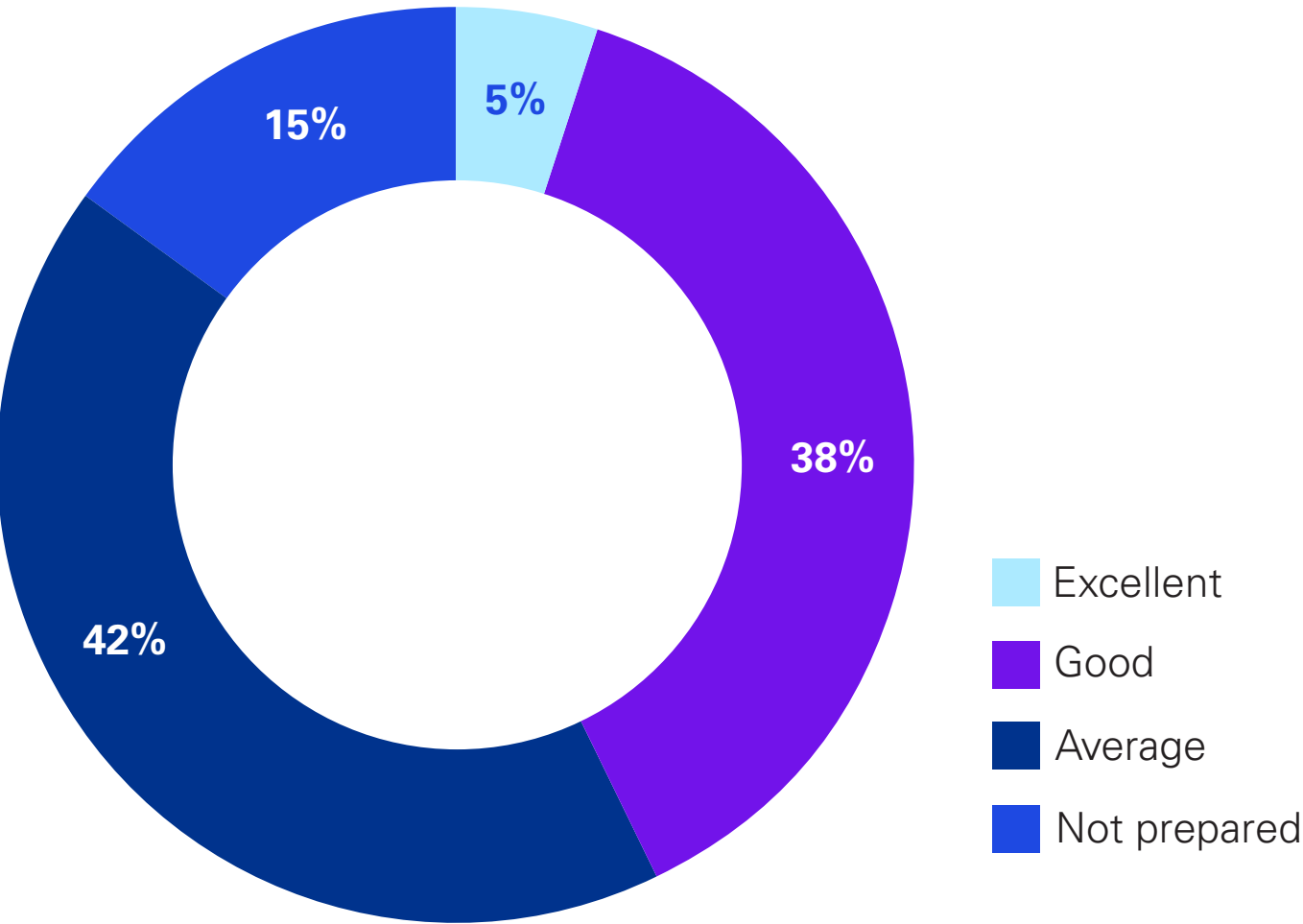
of survey respondents stated that they are involved in all stages of organizational change journeys.

transition programs are a great opportunity for earlier participation by internal audit, from initial planning phase onwards, offering an independent project assessment, to make better use of its discipline in governance and management controls. Internal audit can rationalize responsibilities between lines of defense, to transition manual and detective controls to automated, preventive ones (covering data processing, transaction and accounting, as well as IT general controls). At the same time, internal audit can check to ensure that separation of duties and appropriate access restrictions are in place, to uncover any weaknesses that could lead to unauthorized users entering the system.

Keeping ahead of emerging risks

Just 42 percent of respondents claim to have “excellent” or “good” preparedness for auditing risks associated with emerging technologies like cloud security, AI, ML and blockchain (see Figure 4). One concern is the presence of ‘unknown unknowns’, where audit teams are not aware of risks and consequently fail to include them in audits. As specialists in risk and control, internal audit professionals are uniquely placed to advise the business on how to most effectively cope with the impact of these pervasive new technologies.

Figure 4: How well prepared is your IA team in auditing emerging tech risks?



To cope with a barrage of new technology-related risks, IT internal audit teams should be closely aligned to the business and the risk function, to build credibility and relationships, so that relevant risk information flows through on a real-time basis.

Nicole Lauer
Americas Tech Governance and IT Internal Audit
Leader and Principal
KPMG US



02

Can innovation fill the capability gap?



Assessing technology internal audit capabilities

To navigate the ever-changing landscape of risk, organizations are striving to keep up with the rapid global technological changes. They are doing this by leveraging new operating models that have two aspects. The first aspect involves assessing the current skill sets of individuals within the organization. The second aspect focuses on utilizing the available technologies to enhance optimization and efficiency.

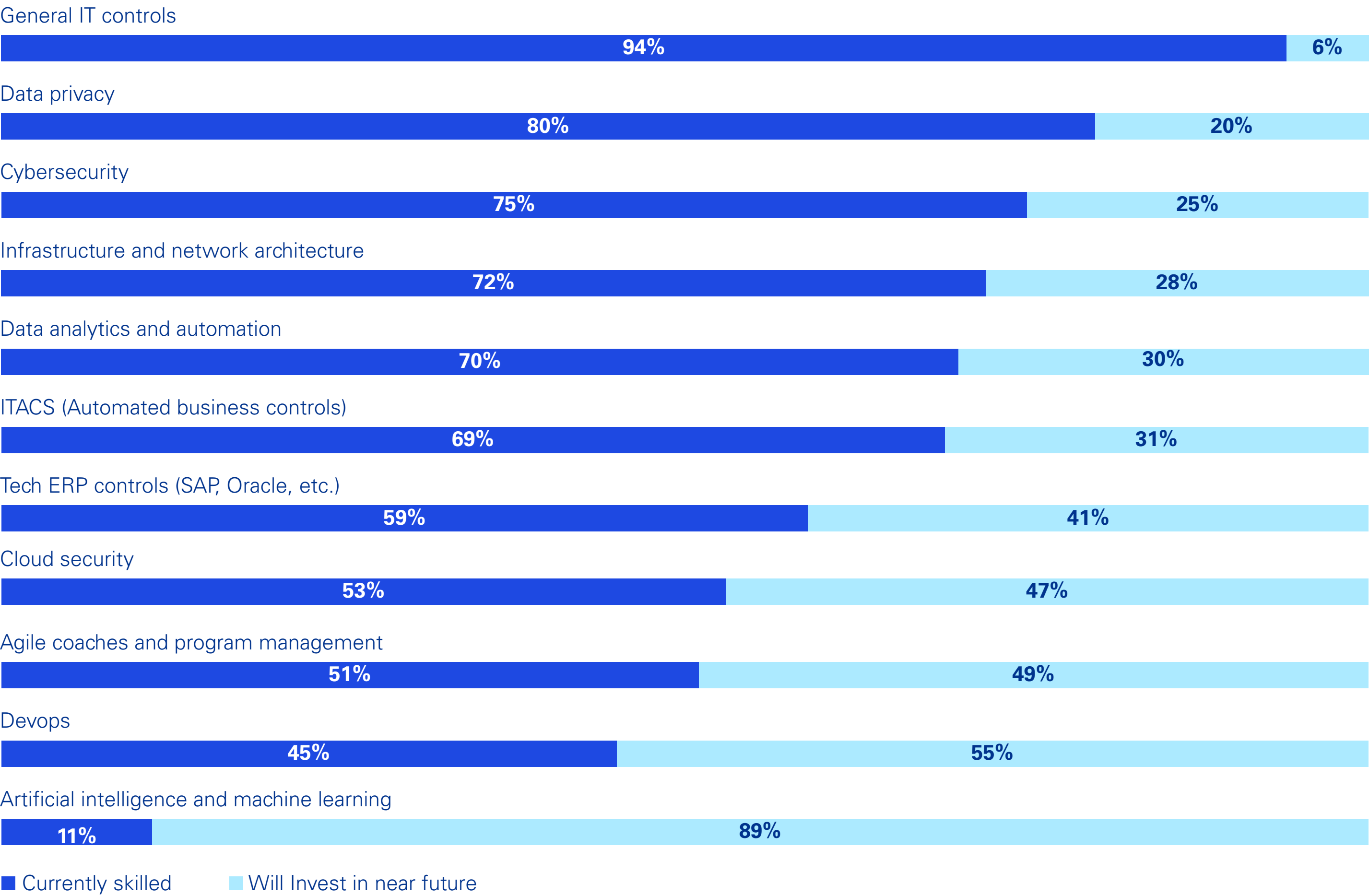
Technology has become ubiquitous, ingrained in everything we do. Yet just one in ten of the survey respondents say that half or more of their teams focus on technology audits. Given that 65 percent of the surveyed organizations have an internal audit team of 25 or fewer members, it seems that only a handful of auditors have a well-defined technology agenda.

But do internal audit professionals have the skills to tackle technology audits? The survey responses indicate there are some clear gaps, notably in AI, ML, DevOps and cloud security (see Figure 5). AI is a particular challenge, with a pace of growth that exceeds most previous technologies. It’s likely that many employees are starting to use AI independently and this could increase data security and privacy risks — as well as inadvertently bringing unreliable information into the organization — calling for stronger governance and guardrails to counter these operational risks.

On the positive side, 80 percent of survey participants say their internal audit functions have data privacy skills. Regulations like GDPR (General Data Protection Regulation) have put pressure on organizations to manage personal data with care and attention.

And, compared to KPMG’s previous years’ IT internal audit survey, twice as many respondents report skills in advanced analytics and automation, with more modest increases in program management, cloud computing and security skills.

Figure 5: Technology audit skills composition



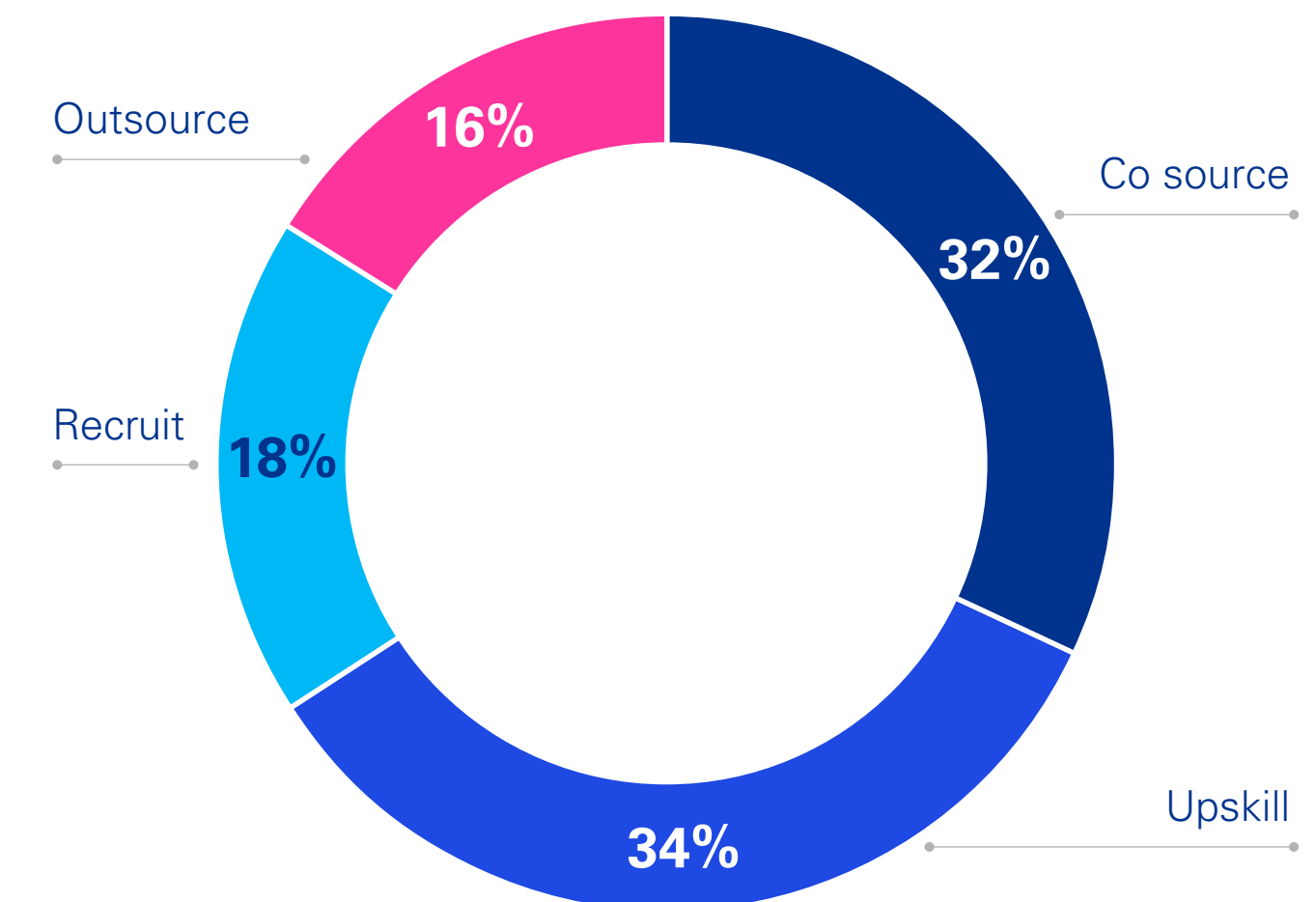


Bridging the capability gap

As the lines between the business and technology audits blur, and integrated audits become more common, all auditors should be upskilling in technology. When working in a single organization, however, internal auditors tend to acquire deep organizational knowledge but often limited technical knowledge and may lack a broader industry or cross industry overview.

When asked how they plan to address skillset gaps, the respondents' most common answer by far is a combination of upskilling and co-sourcing. Recruiting full-time specialists in specific technologies may not always be cost-effective, as these (relatively highly paid) individuals may only be required for certain projects, which could leave them underutilized for some of the time.

Figure 6: What are you doing to address the skill gap?



Internal audit teams must evolve alongside these rapid technological changes. Bridging the skill gap in areas like AI and cloud security is not just a necessity — it's critical for maintaining organizational resilience, especially as these 'emerging' technologies increasingly become commonplace.



Jon Measures
IT Internal Audit Leader
KPMG UK





With budgets expected to be tight, internal audit teams could struggle to hire many new full-time employees, opening the door for more co-sourcing, which brings access to a critical mass of internal auditors, with up-to-the-minute technical skills and extensive exposure to emerging technologies across many audits — something that’s hard to develop internally. Co-sourcing also goes hand-in-hand with upskilling, as the providers can offer training as part of their service.

By understanding the organization’s technology roadmap, internal audit functions can identify future skills needed and work out how to access these capabilities. Training options include vendors and knowledge-sharing communities — as well as co-sourcing partners, who can concurrently carry out ‘heavy lifting’ on the audit execution and help to train in-house teams to become more independent. Learning platforms can also share knowledge and reduce dependency on a few skilled individuals. One essential internal audit skill is report and document writing, which could be enhanced significantly by the use of technologies such as Gen AI, reducing re-work and shortening learning curves for auditors.



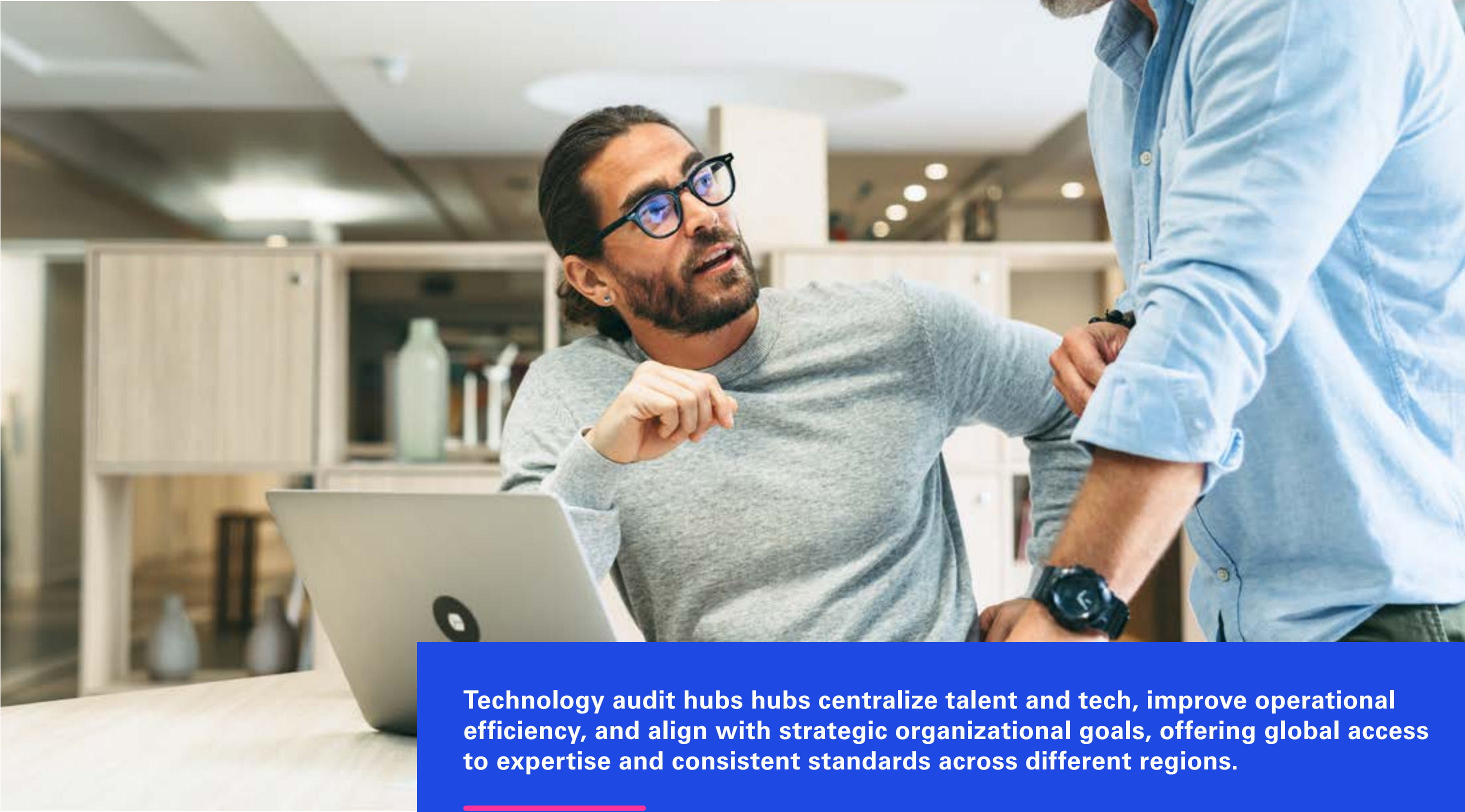
It’s a challenge to keep the internal audit team up to speed with every new technological development. Employing technical specialists with very specific skills may not be cost-effective, as they could be redundant for some periods. A hybrid mix of in-house, outsourced and co-sourced skills is a possible option, as larger external partners can acquire a critical mass of capabilities through their global scale.



Laurent Gobbi
Global Technology Risk Leader
KPMG International



In KPMG’s [Repowering technology audit](#) report, we discussed the exciting potential of technology audit hubs, which are transforming traditional audit functions. They are adaptable to changing business conditions and emerging risks, thereby promoting proactive risk management. Moreover, their governance structure enables better communication and integrated assurance — crucial for decision-making. With feedback loops and a culture of continuous improvement, technology audit hubs have become strategic levers enhancing the efficiency and quality of internal audit functions.

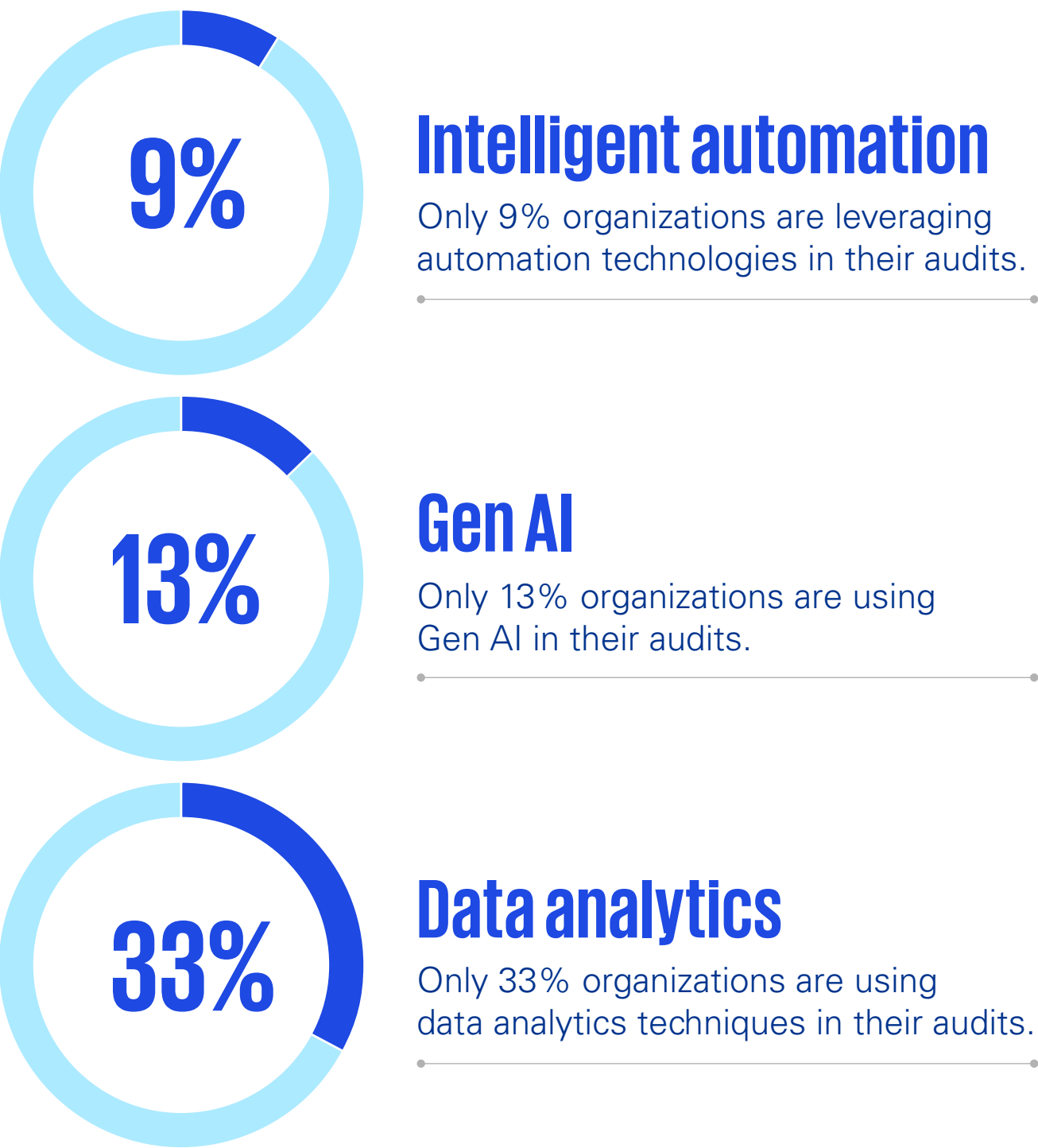


Technology audit hubs centralize talent and tech, improve operational efficiency, and align with strategic organizational goals, offering global access to expertise and consistent standards across different regions.

Embracing new technologies to transform IT internal audit

Despite rising technology audit budgets, efficiency remains a big priority, placing considerable pressure to raise productivity. New technologies offer a route to increased efficiency, by enhancing audits and generating quality reports and work papers. The most commonly used tools are for, data analytics and visualization (33 percent use these in at least half their audits). Intelligent automation and Gen AI feature in relatively few audits — which offers plenty of room for improvement. (see Figure 7).

Figure 7: What percentage of audits are you leveraging the below technologies?



In adopting new technologies, internal audit teams should be disrupting from within — no easy feat when they’re busy planning and carrying out audits. Additionally, there is the challenge of getting access to the right data to feed these various tools, with privacy regulations potentially getting in the way. AI presents a particular problem in that it’s already ‘baked into’ many products, as well as being used independently by employees.

Internal audit teams can benefit immensely from new technologies, but they need solid use cases that demonstrate a positive return on investment — as well as the know-how to get the most out of the tools at their disposal. The business case is not as clear as one may think, when you consider the costs of licensing the tools, cosourcing support and training staff on how to use them.

Figure 8: The potential benefits of Gen AI for internal audit:

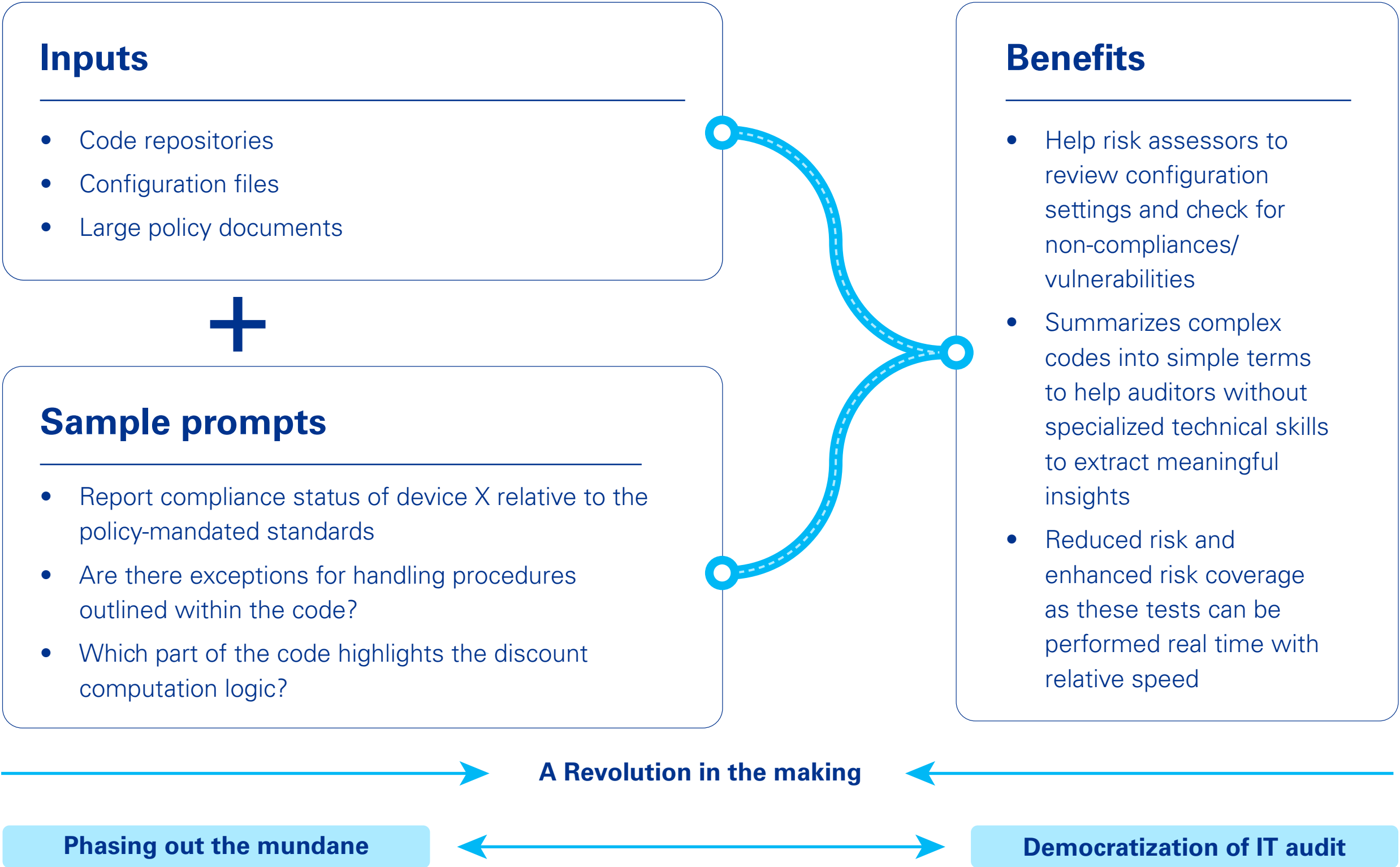
- Discovery and research, document analysis
- Automating complex solutions and processes to ensure compliance with a regulatory standard/industry best practices
- Discovering trends and gaining insights from data through consolidation of data
- Anomaly detection including behavioural analysis to identify deviations
- Automated regression testing, simulation of specific scenarios to identify vulnerabilities in the system
- Improve user interactions through enhanced chat and search experiences
- Less redundancy by automating repetitive tasks in the daily audit workflow
- Greater efficiency by analyzing enormous amounts of input data
- Enables processing and converting complex information (such as configuration files/code repositories) into human readable formats

Generative AI potential in IT internal audit

To get the most out of this exciting technology, IT internal audit should define clear use cases and outcomes.

In Figure 9 below, we show how Gen AI can help internal auditors review large documents faster, enhance user interactions via chatbots and better search capabilities, identify anomalies and vulnerabilities, and automate complex processes to ensure they comply with regulatory standards. All of these tests can be performed in real time at fast speed.

Figure 9: Application of Gen AI in testing technology controls



There are a lot of potential new technologies for transforming IT internal audit processes. While the initial investment may seem substantial, considering licensing, co-sourcing support, and training, the long-term benefits of increased efficiency and quality reporting can't be overlooked. It's clear that the adoption of these technologies, is not just about purchasing new tools, but also about disrupting from within and changing our approach to audits.

Richard Knight
US Technology Internal Audit
Solutions Leader and Principal
KPMG US



03 Technology audit maturity



Climbing the technology audit maturity pyramid

As businesses become more technology-centric, IT internal audit teams need to understand how ready they are for the associated risks and opportunities — and how they can develop the required skills. We observe three stages on the technology audit maturity ladder (Figure 10).

A maturity assessment of organizations participating in our survey placed 49 percent at the Foundational level, 46 percent at the Emerging level, and just 4 percent at the Trendsetter suggesting, considerable opportunities for improvement. (Figure 11)

Figure 10: The technology audit maturity ladder

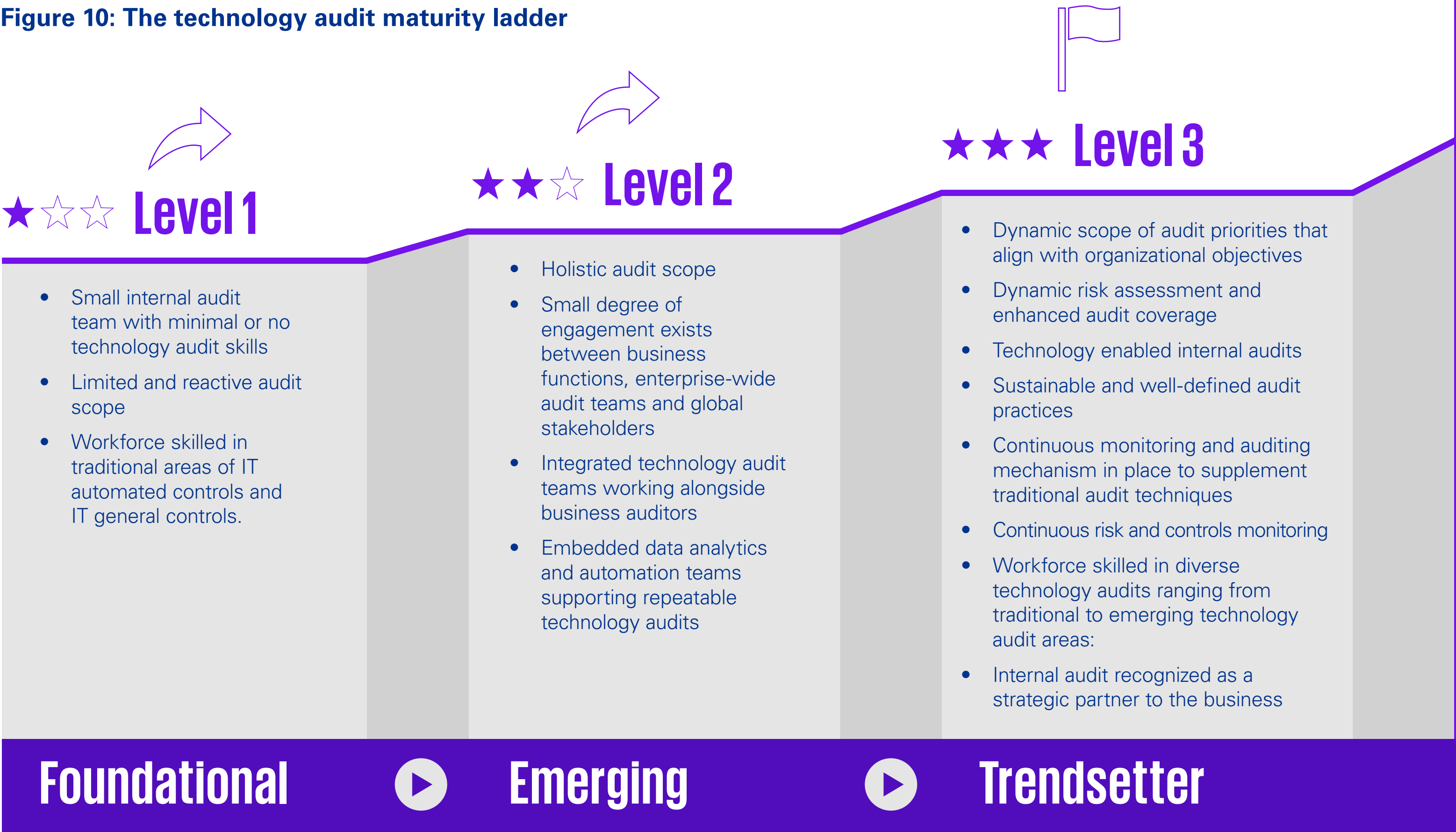
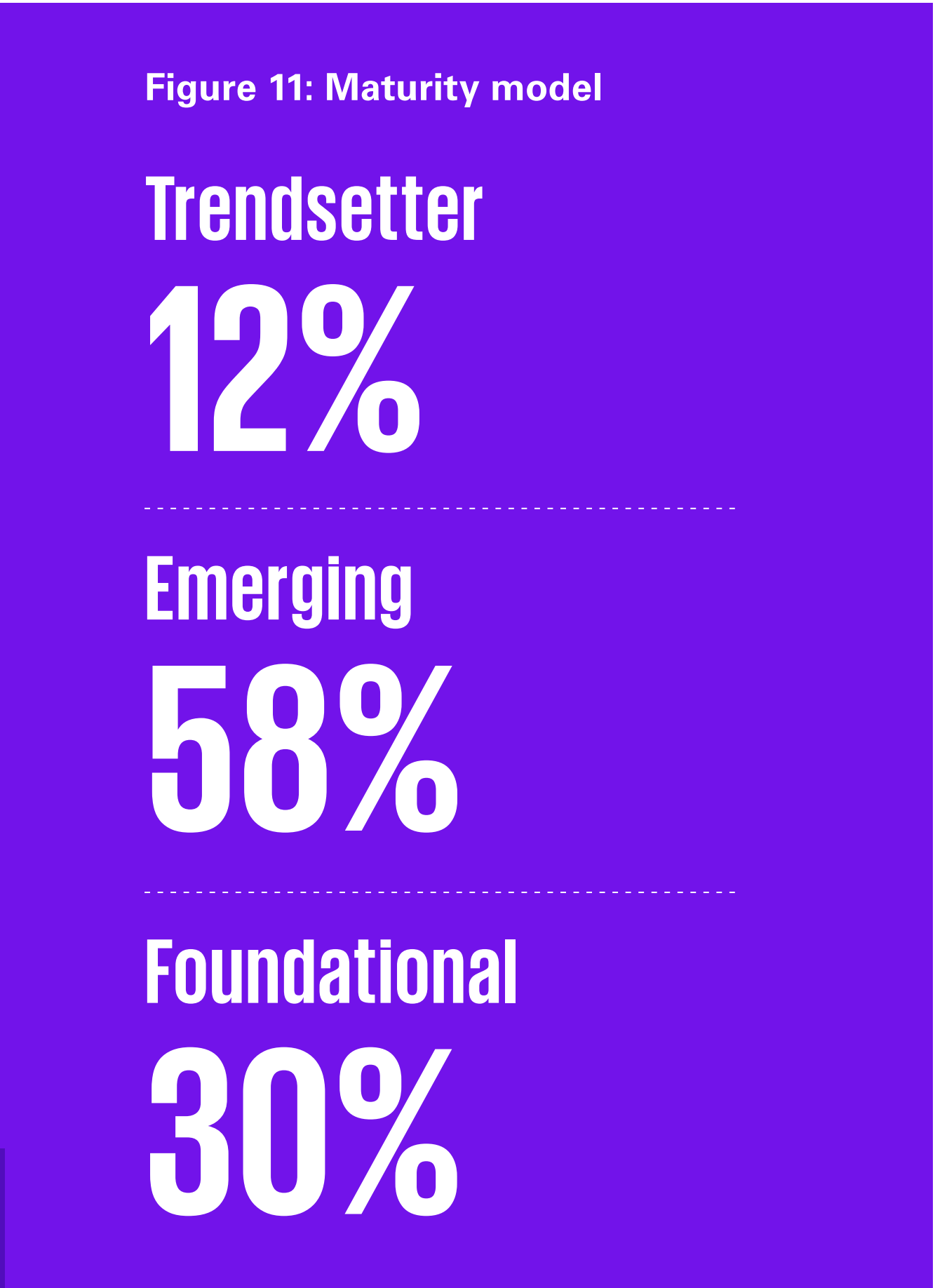


Figure 11: Maturity model



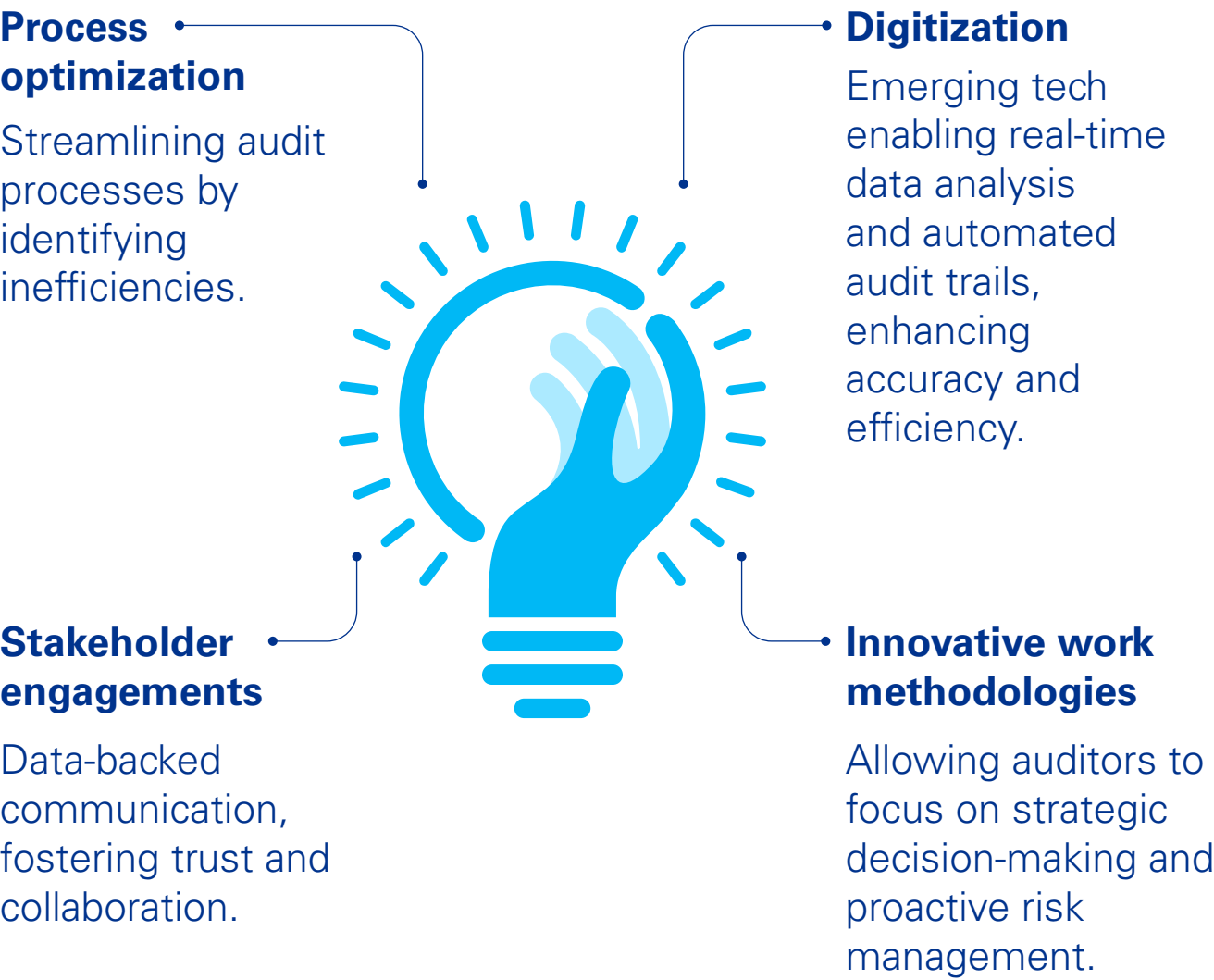
The role of IT internal audit is not just becoming increasingly critical but is at the very heart of the rapidly evolving digital landscape. The challenges posed by cybersecurity, cloud, Gen AI, data privacy, and blockchain are not mere hurdles, but opportunities for innovation and transformation. The need for robust IT governance, compliance, and risk management is not just urgent, but paramount to the survival and growth of organizations in this digital age.

The findings from this year’s report do not just suggest but underscore the pivotal role of IT internal audit in driving transformation, strengthening risk management frameworks, and fostering innovation to improve organizational resilience. For instance, the fact that only 21 percent of IT internal audit teams are involved in ESG assessment or readiness is not just a statistic, but a call to action for the audit community to step up and embrace the challenge.

The fast pace of technological innovation demands an adaptable internal audit function where team members are confident in addressing changing risks — and in using technology to improve performance, via digitization, process optimization, innovative work methodologies and stakeholder engagement. The role of internal audit in enabling the swift, safe and ethical adoption of Gen AI is not just a responsibility, but a catalyst for change. (see Figure 12). Internal audit has an opportunity to achieve continuous, real-time auditing enhanced by visualization, to become an integral part of leadership decision-making.

The maturity assessment of organizations participating in the survey is not just a reflection of the current state, but a roadmap for the future.

Figure 12: How IA is adapting to innovation and risks




The fact that 49 percent are at the Foundational level, 46 percent at the Emerging level, and just 4 percent at Trendsetter level is not a cause for concern, but a testament to the immense opportunities for improvement and growth that lie ahead.


In the face of these challenges and opportunities, the question is not whether we can afford to invest in IT internal audit, but whether we can afford not to.

KPMG professionals are ready to collaborate with you to navigate this transformative landscape. Our expertise in IT governance, risk management, compliance, and innovative technologies such as Gen AI and blockchain uniquely positions us to help your organization turn challenges into opportunities. We can support you in enhancing your cybersecurity measures, ensuring data privacy, and driving ESG initiatives, all while strengthening your overall IT internal audit function.


Explore how KPMG can help you build a robust and future-proof IT internal audit strategy. Together, KPMG can help your organization survive and thrive in the digital age.



The technology audit maturity ladder highlights a critical gap — while many organizations are advancing, few are fully leveraging tech-enabled audits. This is where the future of internal audit lies, as a strategic business partner driving value.

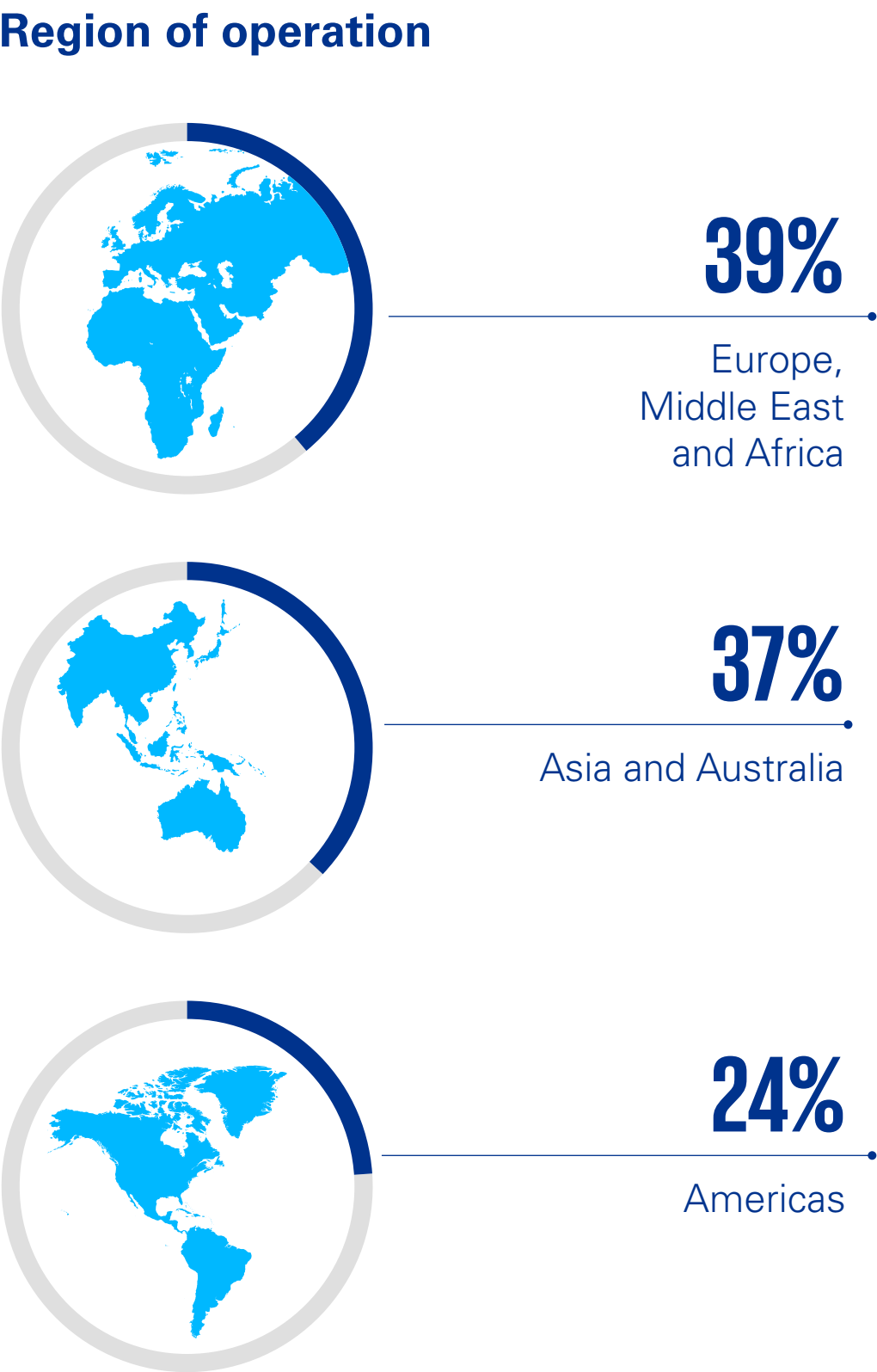
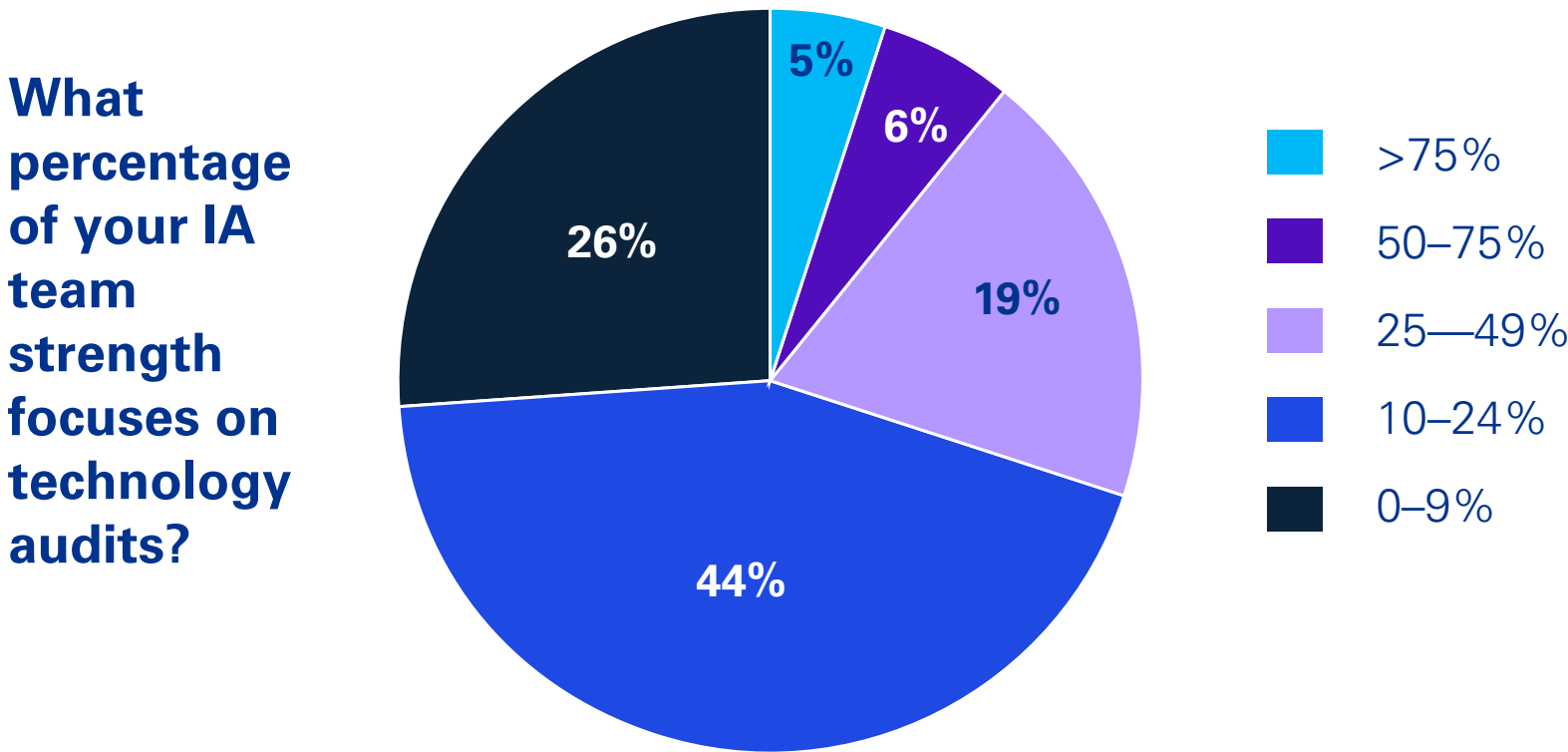
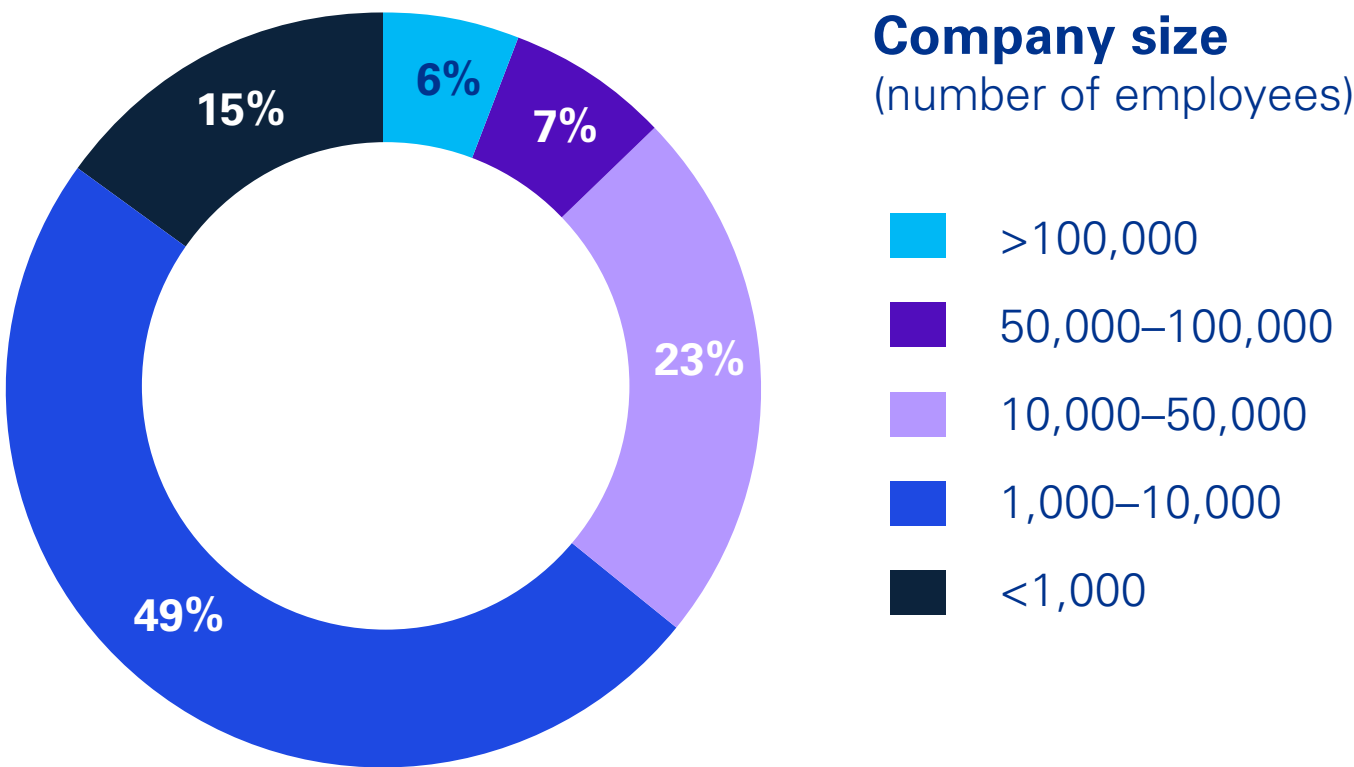


Kareem Sadek
Partner, Advisory
KPMG Canada



Study methodology

The Global IT internal audit survey features the responses from senior executives from diverse industries and localizations.



Explore our related content



[Global IT IA Outlook Report 2023 — KPMG Global](#)



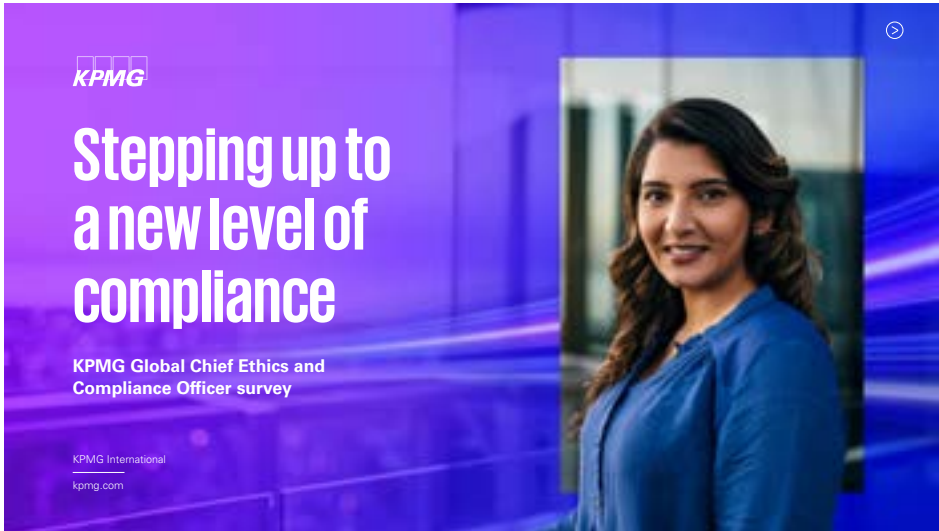
[Internal audit's role in ESG — KPMG Global](#)



[The evolution of non-financial risk — KPMG Global](#)



[The future of IT — KPMG Global](#)



[KPMG Global CCO Survey — KPMG Global](#)



[KPMG global tech report 2023 — KPMG Global](#)



[Controls transformation — KPMG Global](#)



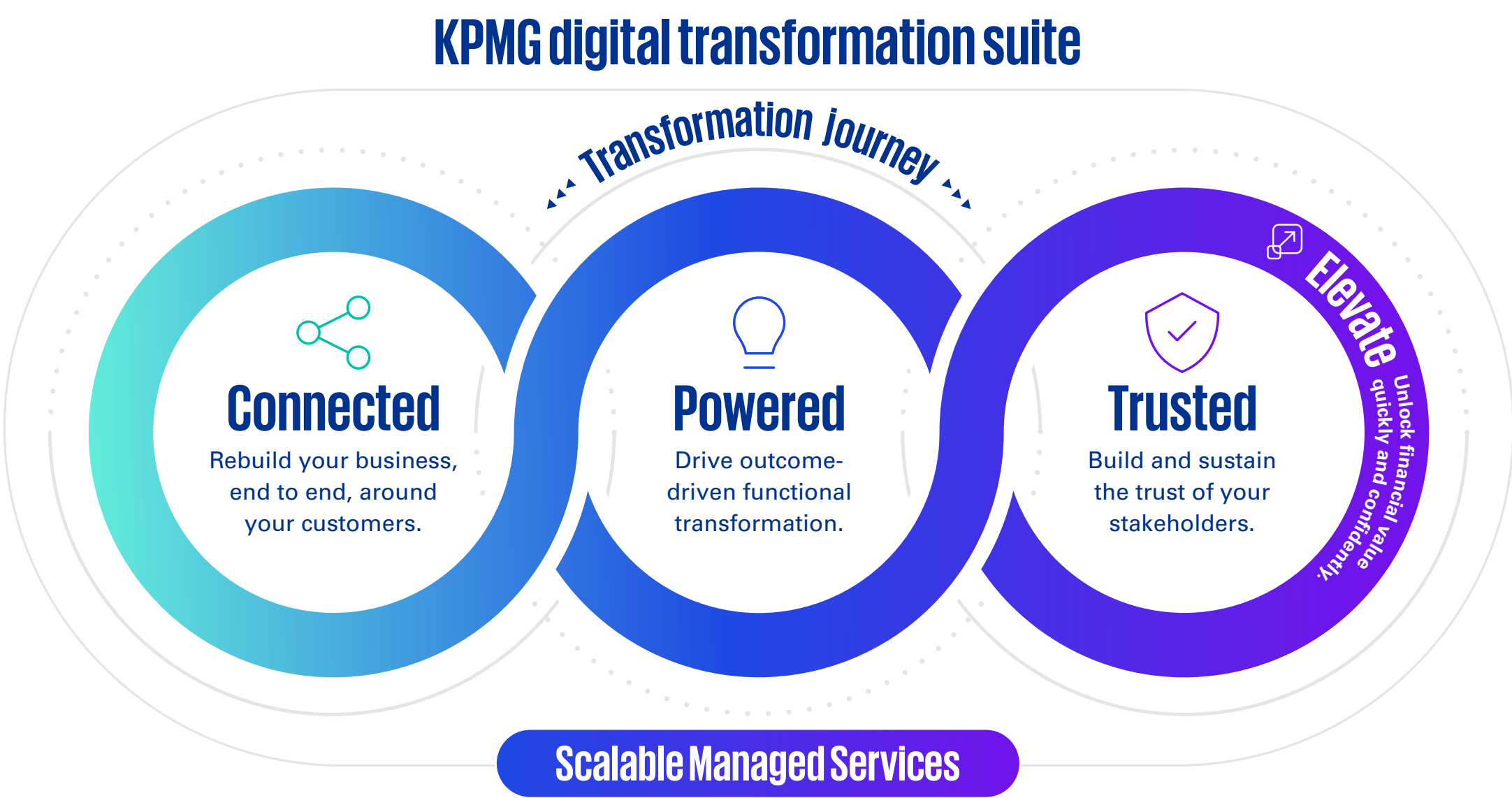
[Transforming Technology Risk — KPMG Global](#)

How this connects to what we do

In today’s dynamic business landscape, the significance of data as the driving force behind organizational operations cannot be overstated. Our reliance on AI and other emerging technologies underscores the critical need for high-quality data to derive insights that fuel innovation, efficiency, and regulatory compliance. We recognize the central role of internal audit teams in ensuring data quality, integrity, and privacy standards are met, thereby facilitating ongoing digital transformation efforts.

At KPMG, our internal audit professionals are committed to addressing threats to organizational integrity. From bolstering controls and ensuring regulatory compliance to conducting meticulous investigations and developing integrated solutions, our diverse team stands ready to safeguard your organization’s reputation and financial interests. Anchored in our efforts is the steadfast commitment to cultivating trust — a cornerstone of sustainable success in today’s complex business environment.

Learn more at: kpmg.com/risk



Transforming for a future of value

KPMG firms’ suite of business transformation technology solutions can help you engineer a different future — where new opportunities are designed to create and protect value.



Contacts



Laurent Gobbi
Global Technology Risk Leader
KPMG International and Partner
KPMG France



Anil KV
Global Leader for Tech Governance
and IT Internal Audit
KPMG International and Partner
KPMG India



Nicole Lauer
America’s Tech Governance and IT
Internal Audit Leader and Principal
KPMG US



James Buchanan
ASPAC Head of Tech Governance and
IT Internal Audit and Partner
KPMG Australia

Acknowledgment

This report would not be possible without the invaluable planning, analysis, writing and production contributions of colleagues around the world.

Alexander Holsten
KPMG Luxembourg

Guillaume Cuisset
France

Lawrence Amadi
KPMG Nigera

Rui Gomes
KPMG Portugal

Andrew North
KPMG in the UK

Harshit Pandey
Global IT IA PMO Team

Luca Boselli
KPMG Italy

Sipho Ndaba
KPMG South Africa

Anjaly Augustine
Global IT IA PMO Team

Jason Dong
KPMG China

Mallika Chandra
KPMG India

Tejas Mehta
KPMG UAE

Carmen Cronje
KPMG Ireland

Jon Measures
KPMG UK

Matt Tobey
KPMG US

Thomas De Backer
KPMG Belgium

Diego Monteleone
KPMG Italy

Kareem Sadek
KPMG Canada

Nirmalya Banerjee
KPMG Switzerland

Florian Magin
KPMG Thailand

Ken Kumagai
KPMG Japan

Richard Knight
KPMG US



Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com



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.

© 2024 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

KPMG refers to the global organization or to one or more of the member firms of KPMG International Limited (“KPMG International”), each of which is a separate legal entity.

KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. For more details about our structure please visit kpmg.com/governance.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Throughout this document, “we”, “KPMG”, “us” and “our” refers to the global organization or to one or more of the member firms of KPMG International Limited (“KPMG International”), each of which is a separate legal entity.

Designed by Evalueserve.

Publication name: Trailblazing digital frontiers | Publication number: 139495-G | Publication date: October 2024