KPMG

Technology risk and its impact on internal audit

Evolution of the practice in Saudi Arabia

July 2024
KPMG Professional Services

Table of content

Introduction

In the context of the rapid digital transformation across Saudi Arabia and the fast-paced global developments in technology – particularly in artificial intelligence (AI), this paper discerns implications of technology on internal audit attempting to highlight common concerns with a focus on the Kingdom.

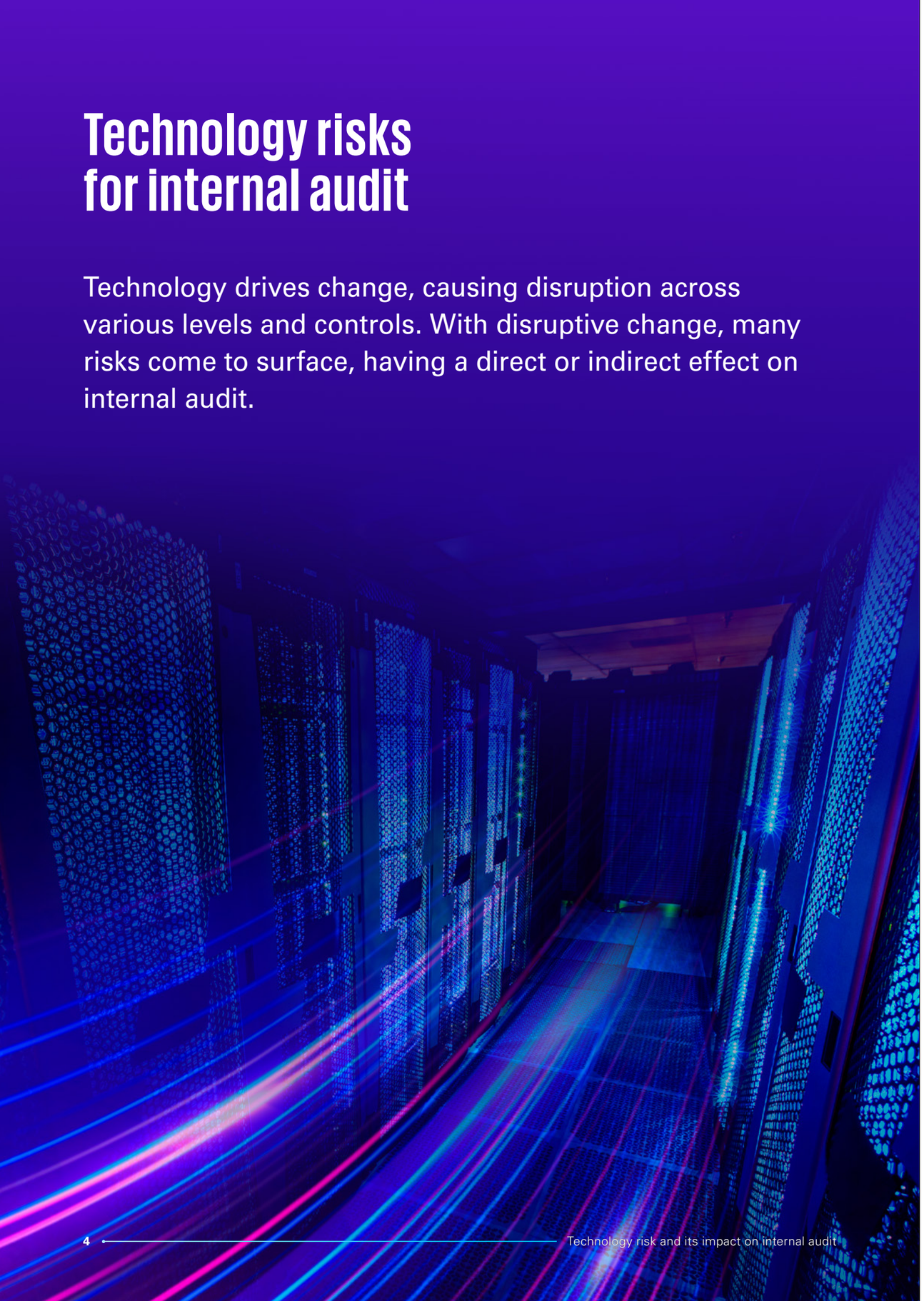
The future of internal audit envisions to move away from manual documentation and testing towards a technology-driven approach that leverages AI. However, with the ever-evolving nature of business and internal control environment, internal audit practices need to adapt with ubiquitous changes. These include rapid technological advancements and evolving regulatory landscapes to ensure providing reasonable assurance over the control environment. By embracing technology and adapting practices, internal audit can remain a critical partner in organizational success.

This paper will discuss various risk factors that technology poses for internal audit practice within Saudi Arabia. It will provide a walkthrough approach to addressing risks that are core components of the Kingdom's digital transformation program, namely data privacy concerns, use of big data, cloud computing and AI. We will explore the impact of technology on internal audit practices and the emerging challenges and disruptive opportunities they bring for the internal audit function in both the near future and the long run.

Khalid Yasin
Partner, Head of Enterprise Risk Services
E: kyasin@kpmg.com

Technology risks for internal audit

Technology drives change, causing disruption across various levels and controls. With disruptive change, many risks come to surface, having a direct or indirect effect on internal audit.



With the significant influence from technology, the profession's regulatory framework has been extensively reshaped to address the emergence of technology-driven risks. This includes an increased need to adapt to technology and its evolution within the enterprise environment, while maintaining a high level of integrity and governance in the assurance services it provides.

Technology helped reshape modal structures, core processes and this changed the way things are done.

What worked in the past no longer works today, as technology's repercussions have been pervasively implemented to reshape matrices and workflows in a systemic manner.[1] While technology places internal audit at the forefront of many novel risks, the main risk it has is internal auditors not knowing enough about technology itself.

With an exponential leap into the digitalization of workflows and process mapping, internal auditors are not only concerned with adding value through risk assessment, but also preserving value by ensuring ethical considerations and proper controls are implemented amid fast-paced workflow changes. Therefore, internal auditors need to possess a thorough understanding of the management's direction and dynamics of the organization's industry to not only provide assurance on controls effectiveness and operational efficiency but also weigh the impact that any risk from technology may have on the long-term objectives.[2]

This shift has fueled numerous entrepreneurial initiatives and family businesses from and across the internet. Even established businesses and banking institutions are embracing online models, with some going fully digital.[3]

In today's digital age, as businesses increasingly operate through digital platforms, they rely heavily on technology in the enterprise architecture and solutions they offer. This digital shift has led to a significant amount of corporate and personal data being used, processed, and stored online.

As a result, leakage of non-public and material information became a primary focus for regulators seeking to protect the public from cybercriminals. Data privacy – which is heavily exposed with technology systems such as servers and cloud storage -is something internal auditors are on guard for. [4]

A constant need exists to address data security concerns.

In the case of most emerging technologies, core process variables are enabled through the sharing, storage, and use of data online, on public networks. Without appropriate controls and safeguards, the data can be accessed by unintended and unauthorized users.

The concern grows with technologies such as the Internet of Things (IoT), where in some instances, the entire ecosystem is accessed remotely whilst peripherals and devices store data. Another technology that presents challenges is AI with the use of open data platforms and has been identified as a priority topic by the government for the threat exposing data privacy on such platforms.[5] As many AI platforms rely on Large Language Models that use vast open data sources, private information and sensitive data can be tampered with and improperly used, such as biometrics saved digitally. This poses a significant risk to personal data privacy – a concern that internal auditors rightfully uphold.

In the light of national efforts directed to safeguard the Kingdom's information and communication technology infrastructure and storage systems, new laws have served such initiatives thereof.[6] Internal auditors are hence considering this factor to ensure organizations operating within the Saudi legislation are abiding to such regulations. For example, the storage of Saudi-owned data must be stored on cloud services that are not remote, but physically located in the Kingdom. The strategic vision is in its implementation phase, with giga-projects integrating emerging technologies, like Alibaba Cloud establishing a presence in the Kingdom mainly for establishing hosting servers as a step to protect Saudi data from any breach or potential information leak.[7]

Authorities are more than ever committed to ensure a proper data retention system and internal auditors are ensuring organizations fully comply with this aspiration. The type of data to be covered by automation, the rights and privileges to access data, and the intended purpose of information are all parameters in place to protect users and corporations from the use of data in unintended contexts or motives. This is in congruence with AI being integrated in megaprojects and its implementation set in giga projects like Neom, where visionaries seek to integrate robotics and AI into every aspect of citizens' lives. AI is needed for this, as it would allow the Saudi state to leapfrog industrialization and shortfalls in state and institutional capacity.[8]

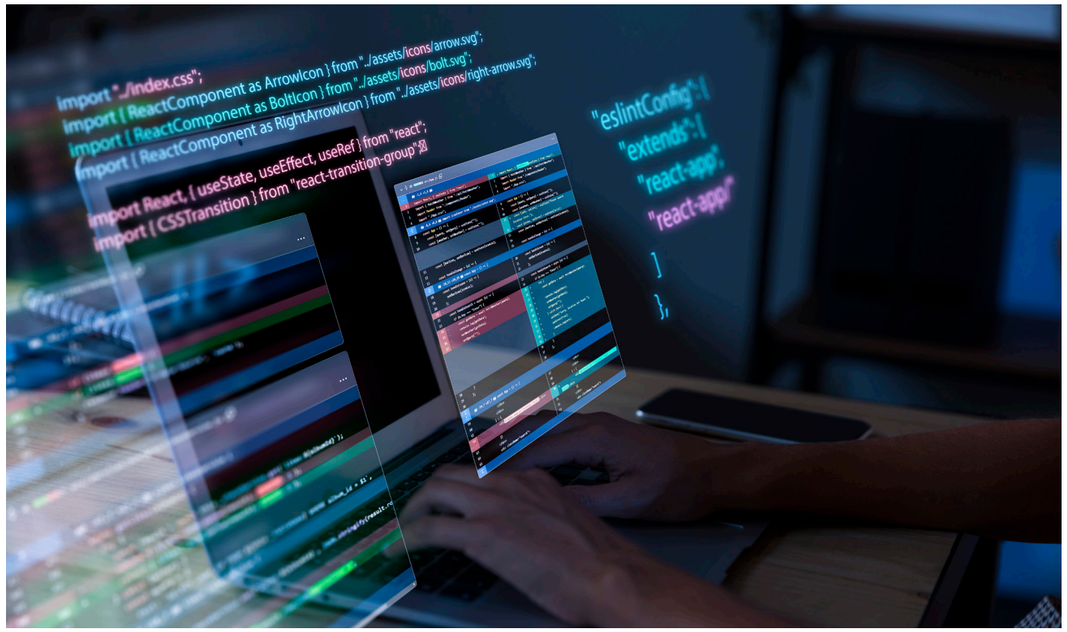
Information technology plays a growing role in modern auditing.

For instance, the extent technology is being used across multilayered process within an organization compared to the maturity of its IT control environment may also suggest a risk for internal audit. This connection is explored through recently conducted research, which is facilitated through Computer-Assisted Audit Tools and Techniques (CAATTs). The logical paths and relations established through the gathering of empirical data suggest that for work processes that are highly integrated with technology and automation-enabled, a high CAATTs usage can yield positive results where its application can be effective. One might highly expect IT-knowledgeable internal auditors to rely less on CAATTs; however, research suggests this is only true when the application of CAATTs is not as effective.[9]

By default, most AI-based software applications currently in use follow a predictive AI model and are based on human-inputted algorithms and data. Few technologies in use rely on generative AI (GenAI) which may potentially "think outside the box" and offer groundbreaking solutions. Although it is quite novel, SDAIA issued guidance for using, analyzing, and implementing generative AI by proposing principles for responsible use, and presents recommended practices for both Government and Public use.[10] Internal auditors, at their own discretion, need to understand which type of technology is being used to adequately address the drawbacks it has as well as knowing which guidelines and measures are meant to be relied on as reference material.

Nevertheless, internal auditors are still unable to fully limit the aftermath that may be caused from technology or even, ultimately, predict how best to address it. Although using technology as a tool to deliver their mandate, systems currently used by internal auditors are not technology-smart, more so, still people-driven. Major applications are archiving systems only, used by internal auditors as tools to shape up, organize and process data. This implies not having reached optimal efficiency to leverage big data with self-running engines to enable continuous monitoring and proper integration of data analytics in the overall automation process of the internal audit activity. Currently, the software that is used largely consists of tools to extract and access data rather than intelligent AI-powered solutions.

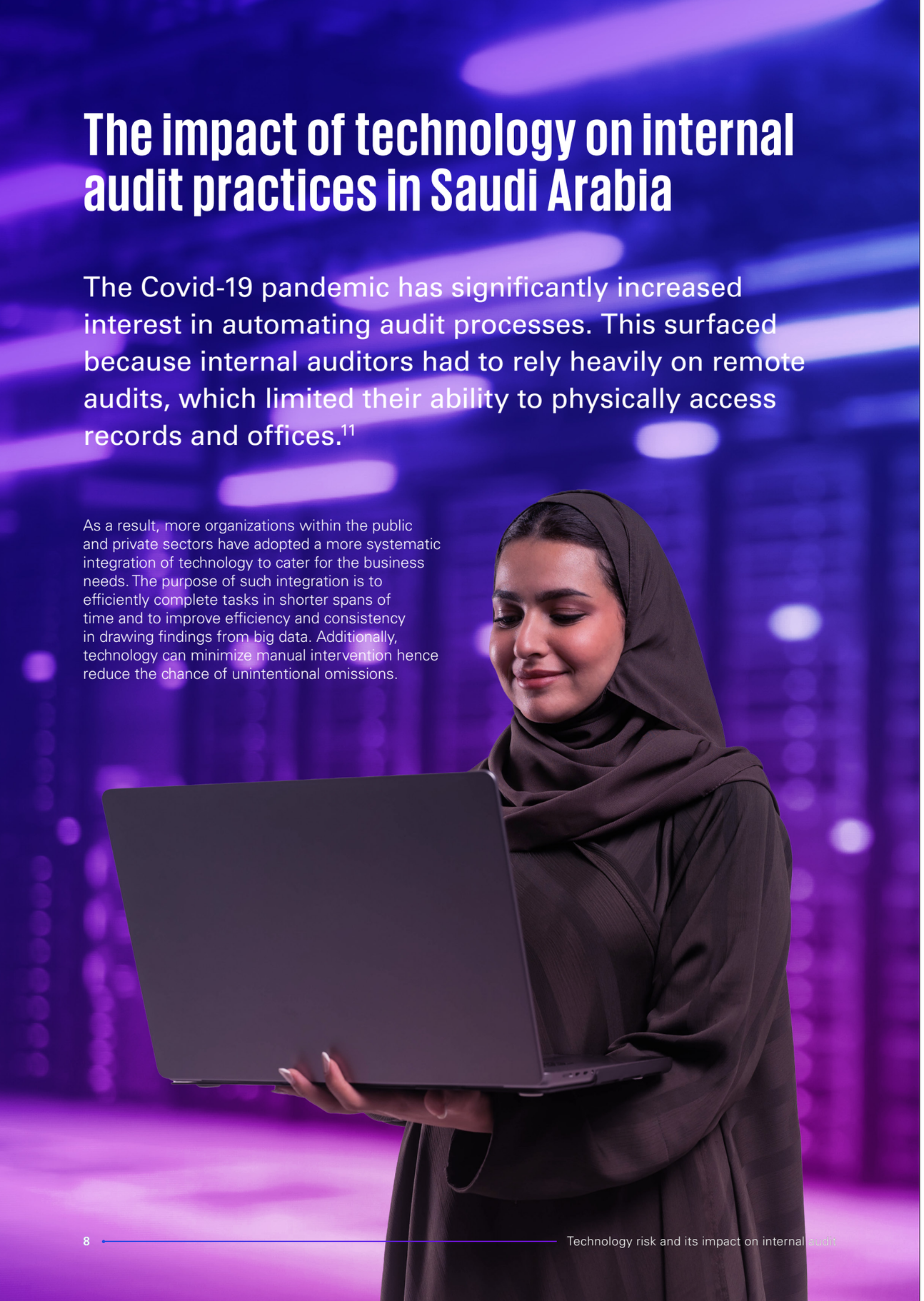
In the following part, experienced internal auditors will offer a walk-through trajectory. They will focus on the main hurdles encountered; key learnings gained while delivering the mission of internal audit in a transformational work environment. This stance acknowledges that the internal audit practice is undisputedly affected by technology's impact. It emphasizes the need for internal audit to cope with the variations, enhancements and implementation driven by the digitalization movement.



The impact of technology on internal audit practices in Saudi Arabia

The Covid-19 pandemic has significantly increased interest in automating audit processes. This surfaced because internal auditors had to rely heavily on remote audits, which limited their ability to physically access records and offices.[11]

As a result, more organizations within the public and private sectors have adopted a more systematic integration of technology to cater for the business needs. The purpose of such integration is to efficiently complete tasks in shorter spans of time and to improve efficiency and consistency in drawing findings from big data. Additionally, technology can minimize manual intervention hence reduce the chance of unintentional omissions.

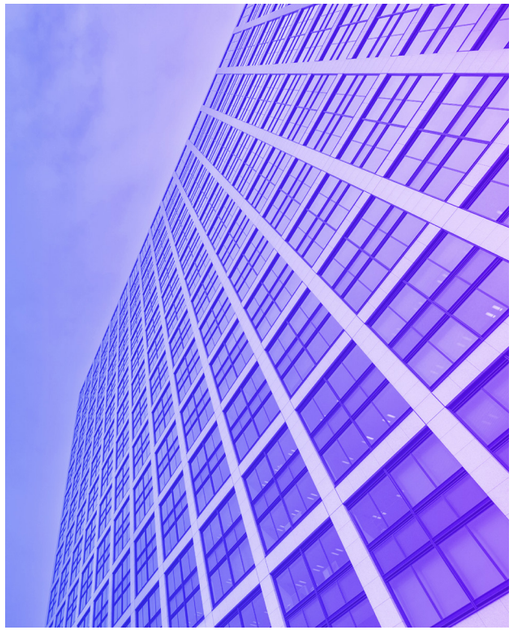


Regulatory bodies like the Saudi Central Bank (SAMA) and the General Bureau for Auditing (GBA) are scrutinizing the impact of technology on business processes. They expect internal auditors to identify and address technology-driven risks. Traditional approaches are no longer sufficient. Governance boards demand a more proactive role from internal auditors and GRC professionals. They need solutions to mitigate technology risks and leverage them for better outcomes. Ultimately, the mere detection of risks and loopholes relating to controls effectiveness and process efficiency is no longer accepted. Internal auditors are now heavily involved in providing assurance as well as solutions to use technology risks as a strength which would eventually translate into reward diligence programs geared towards achieving institutional objectives. With operating systems relying on the extensive use of technology settings, internal auditors are expected to identify what constitutes a system error, a clerical accidental error and an intentional manipulation implying fraudulent intentions. Identification and categorization of such risks is accomplished through an in-depth understanding of operating systems and IT-backed controls whereby prudent internal auditors can manifest the running of simulation scenarios and piloting tools to perform root-cause analysis through proper cross-checking of data. Therefore, addressing the problem from its root case can be substantiated only by possessing an acute knowledge about information technology governance.[12]

Due to adaptation of technology within organizational structures, assurance providers have seen a shift in the role of internal auditors and the practices they go by.

The Saudi Organization for Certified Public Accountants (SOCPA) is a strong advocate for ensuring a smooth transition of workflow and recognizes the role of collaborative work to achieve the highest potential for each process, where such potential is only achievable through maintaining a transparent and effective knowledge transfer scheme. According to the Information Systems Audit and Control Association (ISACA), for internal auditors to keep pace with an accelerating technology curve, they are bound to create greater collaboration between the internal audit and IT teams. The ongoing partnerships between IT and risk management units which surged from 55 percent in 2019 to 79 percent in 2020 indicates the existence and significance of such practice.

In the era of big data, the ability to access and process substantial amounts of information is crucial for effective internal auditing. Emerging technologies in Saudi Arabia facilitated access to data as well



as accelerated the phases of acquisition and processing. Such a phenomenon has been noted through the increase in the number of corporations using big data, such as neo-banks and nano-finance institutions. Saudi neo-banks such as Meem and Hala are payment servicing solution providers that enable monetary transactions on the go and do not grant credit facilities or financial instruments to their users. Nano-finance refers to transactions where monetary operations such as loans, discounts, repurchases are made to individuals with no fixed assets held as collateral, where most records and schemes are maintained digitally.

Digital platforms have made substantial data available and internal auditors are using technology to assist in navigating and analyzing reported data. Mainly, scrutiny on documentation is now enhanced through effective use of powerful tools like data analytics and the process of continuous auditing. In comparison with general information technology systems, where each process and task are the closest thing to siloes, continuous auditing looks at the business process as an architecture comprising indicators, signals that are all linked and integrated around a live-status timeframe.

The digital transformation in the Kingdom is accelerating with emerging technologies like AI and cloud computing taking center stage for businesses.

In the healthcare sector, AI-powered chatbots and virtual assistants can provide round-the-clock support, answer patient queries, and offer personalized healthcare information, which all contribute to an enhanced user experience.[14]

In line with the Vision 2030 to become a leading digital economy, the Kingdom has witnessed a surge in technology use across all sectors and government functions. Technology is now an integral part of every aspect of government operations.

Internal auditors integrate technologies to identify and prioritize risks by ratings evaluated against likelihood and impact, and such technologies are deployed to perform the heat mapping of risks identified for a clearer visualization.

The value delivered by internal auditors is closely monitored by various internal stakeholders – i.e., the auditees and the second line of defense (board of directors, trustees, and audit and risk committees) as well as by the external stakeholders (authorities, regulatory and oversight boards).

Consequently, internal auditors are required to convey to senior stakeholders such as executive management, concise, time-conscious observations, and recommendations. Hence the use of appropriate visuals achieved with technology has enhanced the presentation of relevant substantive data. In fact, better representation of findings promoted the overall experience for audit clients (internal and external) as well as for auditors who can navigate through extensive data – process, report and present it in efficient manners.

Internal auditors within Saudi Arabia are leveraging technology to make their work more impactful. By understanding how technology is affecting the governing architecture and operational model, internal auditors are gauging tech-led parameters to support their fieldwork and testing activity. This includes activating appropriate control measures over IT commands in a way that enhances the audit activity such as timesaving and enhanced sampling techniques. Using technology as a tool for internal audit has improved effectiveness and can therefore benefit the nation at large by being aligned and helping activate its planned digital transformation objectives.

Another emerging technology in high demand by businesses in Saudi Arabia is cloud computing which enables users to use computer system resources with data and enterprise systems being stored digitally on a cloud server and not stored or managed directly by the user.

It is worth noting that among the strategic goals to activate a digitally capable ecosystem, the ICT investment framework – supported by cloud computing – has played a spearheading role as an enabler of cost optimization and value maximization to ensure sustainability with an emphasis on re-using shared capabilities across the government with the aim to reduce duplication of efforts.[15] Such an operation model contributes to building shared capabilities and resources to drive down cost and overhead. In 2021, the stake of deals pertaining to cloud-computing in Saudi Arabia exceeded US$1.7 billion.

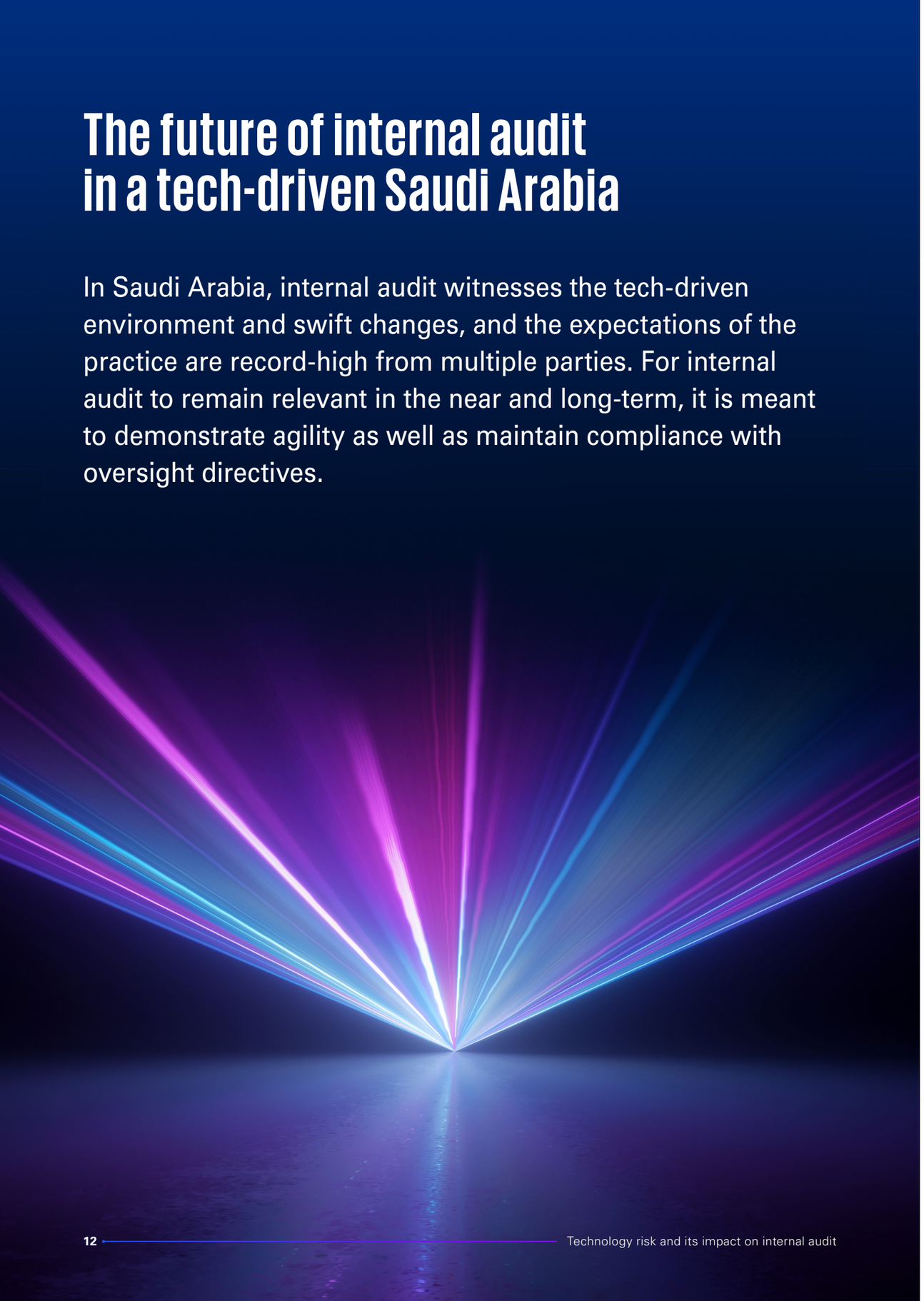
Also, blockchain technology, defined as a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network, has marked considerable growth while being an intuitive medium of transaction.[16]

The use of innovative technologies is undoubtedly effective and efficient, but like any process, it is prone to error. This necessitates constant compliance checks to ensure proper oversight from authorities like the Communication, Space and Technology Commission (CST). By rolling out initiatives and programs, CST maintains its efforts to develop a culture that promotes adherence to safely using information through emerging technologies.[17]

While technology may expose businesses to unforeseen risks and unfavorable events, particularly through open-source platforms and systems operating with non-encrypted controls, it also plays an accelerator role for the internal audit purpose. With high levels of automation and adoption of data through cloud storage systems, the task of internal auditors to gather data is faster than conventional data collection. Previously, obtaining documents relied on process owners to mobilize entire teams to furnish requested data which could take weeks depending on the documents requested, whether these were locatable due to the downfalls of human intervention and errors associated with it thereof.

The future of internal audit in a tech-driven Saudi Arabia

In Saudi Arabia, internal audit witnesses the tech-driven environment and swift changes, and the expectations of the practice are record-high from multiple parties. For internal audit to remain relevant in the near and long-term, it is meant to demonstrate agility as well as maintain compliance with oversight directives.



In a clear objective to combat threats surfacing from technology, regulatory bodies under the patronage and scrutiny of the highest oversight authority prioritize responding to data server breaches, organized anti-money laundering activities, and other forms of cybercrimes.

Saudi Arabia has established a robust regulatory framework for internal audit. Several authorities, including the Saudi Organization for Chartered and Professional Accountants (SOCPA), include proper guidance in circulars and memorandums through which they enforce and enact internal controls specifics and adequate risk management practice, which these, are usually inferred from standards.[18] This guidance helps internal auditors navigate their compliance journey. Official regulatory boards such as SOCPA define the accounting principles internal auditors must adhere to while providing assurance over financial statements accuracy and reporting standards.

The General Bureau for Auditing (GBA) also plays a crucial role by issuing updated guidelines to meet the country's aspiration for sustainable and ethical transactions. These guidelines empower internal auditors to deliver comprehensive assurance services under the Kingdom's legislation and serve the public interest by fostering ethical practices. The Institute of Internal Auditors – Saudi Chapter (SIIA) further contributes through enriching programs and bootcamps to ensure internal auditors are aware of the most recent changes and regulatory objectives. On top of its guidance role as an information hub and databank, the SIIA promotes innovative practice onto how to perform full internal audit cycles while adapting to changing environments. For instance, the IIA signs a memorandum of understanding with the newly formed Arab Confederation of Institutes of Internal Auditors (ARABCIIA), which SIIA is an affiliate country member, to promote collaboration which among various objectives helps increase the level of awareness of internal auditing standards and the techniques and methods of their application.[19]

For instance, the General Data Protection Regulation (GDPR) and similar regulations around the world prioritize responding to data server breaches, organized anti-money laundering

activities, and other forms of cybercrimes. To this end, the Saudi Data & AI Authority (SDAIA) enforced a comprehensive data protection law.[20]

While the legislation requires all government entities to comply with directives and regulations set by the National Data Management Office (NDMO), some businesses still fail to adhere to these data privacy and security policies.[21] Internal auditors uphold highest level of integrity and exert skepticism with regards to data reporting, storage, safety, and security to determine, identify, and potentially detect privacy breaches and leaks of confidential information.

SOCPA requires fellowship holders to pursue continued professional development, including considerations for understanding information technology and general IT Controls (ITGC) as outlined on the organization's official electronic resources.[22] Internal auditors recognize the critical importance of technology and understand that core proficiency in operational effectiveness and financial risk management is no longer sufficient to fully contain technology-related obstacles. Preventive controls aim to stop errors before they occur, while detective controls identify and report errors promptly. Internal auditors focus on providing reasonable assurance and developing recommendations for these controls, which often rely heavily on technology experts.

While having stronger aspirations to strengthen their functional knowledge about technology, internal audit department managers and capability leaders are increasingly focusing on containing tech-related risks by increasing their efforts in the recruitment of non-core audit professionals, particularly operational and financial auditors with IT expertise, or even to the extent of headhunting application developers, cybersecurity experts and programmers to complement their talent pool.

In this context, the practice of internal audit has in itself become more innovative. Adaptive characteristics include reformulating internal audit programs and adopting innovative testing tools such as data analytics, to assess a wider range of controls and variables. In this aspect, internal auditors are looking for practices that foster data curation, analysis, and provenance tools to enable companies to detect data and algorithmic bias. Additionally, internal auditors are to check the veracity of data, tools for explaining the output of an AI algorithm, and tools for performing AI audits to check that algorithms are doing what the companies claim they are supposed to be doing. Such tasks require internal auditors to have the necessary agility in adapting to changing environments. Especially in instances whereby contextual changes precede guidance from oversight authorities, internal auditors are counted on to work autonomously and to come up with effective solutions.[23]

With the integration of technology in the controls architecture and process design as well as real-time values with systems being updated quasi-instantly, auditors can make sense out of reports that are extracted on the spot with real "live" data. As such, "same minute" data is more significant than information included in outdated reports only indicative of the organization's financial health as at the last cut-off date, normally last financial quarter.

For auditors, it is critical to obtain greater clarity and broader visibility on the risk universe, in which they can subsequently gauge and customize the parameters to assess specific variables and contingencies. Such possible options offer unsurpassed insight over risk assessments making them well-defined and neatly structured. For example, technologies like robotic process automation (RPA) automate manual tasks such as migration of data, performing repetitive commands and reconciliation between data sets. With technology being appropriately used, the cross-referencing activity has been considerably eased and simplified in comparison to being time-consuming when performed manually. Although with such technology audit activity can be executed at an accelerated pace, it remains the responsibility of auditors to verify the accuracy of results derived and findings reported.

While disruptive changes are underway, wide implementation of technology comes with a price, and strong guidance to do things right is critical. The Information Technology Governance Framework in Saudi Arabia sets the general standards of which core elements to include and the practice to follow. Authorities like the National Anti-Corruption Authority (Nazaha) have now reached a thorough understanding of such threats caused by technology and are carrying out high scrutiny to control any non-conforming practice.

However, specific guidance can vary between organizations depending on the nature and materiality of data collected, frequency of use and depth of the integration level.[24]

Effectiveness and innovation are also becoming key performance indicators (KPIs) of internal auditors. Professionals are required to bring new solutions to the table, where businesses would reach the same or more targets in shorter timeframes.

This said, to cater for a steady career progression and consistent professional development, continuous learning became a priority for internal auditors to pursue.

Conclusion

The noted impact technology has on organizations in Saudi Arabia opened new horizons for the consideration of internal auditors. With the use of a mature IT infrastructure, appropriate governance frameworks, and powerful tools like data analytics and continuous auditing, internal auditors can effectively classify and assess large data files.

Technology has inevitably impacted the internal audit function, unlocked vast opportunities while also brought new risks to the surface. The rise of emerging technologies placed auditors in a sensitive position whereby they now lead a multifaceted battle to keep the function's purpose in order. Key risks associated with technology include:

The fast-paced changes in the control environment
This is making the challenge record-high for internal auditors to keep up with.

Higher expectations from the stakeholders
Senior management, boards and committee members as well as regulatory authorities are more versed in technology paradigms and expect internal auditors to have a strong understanding of tech-related risks.

Skill gaps within internal audit teams
While some internal auditors are lacking the skillset needed to address broad ranges of tech-related risks in general, internal auditors who are tech savvy still have considerable areas of improvement. Emerging technologies are a step ahead from auditors and continue to provide learnings.

However, technology breakthroughs have added value to the internal audit function. These include:

Re-orchestrating process mapping in well-organized algorithms
Consistent algorithms across the various operational systems that are used make it easier for internal auditors to locate information, and to retrieve and analyze data.

Using technology for deeper insights, agility, and value-added contributions
When used appropriately, data analytics and continuous controls monitoring provide internal auditors with insights, agility, and value. These are just a few examples of tools that can enhance the internal audit process.

By embracing technology and continuously developing their skillsets, internal auditors can ensure they remain relevant and provide valuable insights to their organizations.

Internal auditors, throughout the risk assurance journey, are also performing their validation pre- and post-fieldwork phases in close coordination with the IT department to understand whether such process workflow, insertion or modification of IT internal controls is feasible and what are the main repercussions that may unfold if they are applied or adjusted. In addition, close coordination with legal affairs units helps mitigate the chances of any recommendation provided by internal auditors exposing the entity to significant risks and ensures compliance with the latest regulations stipulated.

KPMG's commitment

KPMG recognizes the significant impact of technology on internal audit. To address this, we are committed to equipping our internal auditors with the latest techniques to overcome challenges widely common in the fast-paced environment. For instance, we are dedicated to upskill our internal auditors by transferring key skills, methods and learning through various sessions ranging from bootcamps to interactive trainings and collective workshops. Knowledge transfer in this regard is enabled through a combination of self-paced online modules and instructor-led classes.

Living up to its pledge of being a trusted professional services firm, KPMG goes beyond this oath by continuously training its staff to meet client needs and adapt to the ever-changing market demands shaped by technological advancements. Leaders curate periodically training materials including articles focusing on specific technology trends relevant to internal audit. Thought leadership publications like these are the testimony of this research as well as the product of our professionals' key learning journey.

References

[1] isaca.org, 2023
[2] The Changing Role of Internal Auditing Function in Organisation, 2022
[3] dga.gov.sa, 2023
[4] bigid.com, 2023
[5] ai.sa, 2024
[6] Personal Data Protection Law, 2021
[7] Vision2030.gov.sa, 2021
[8] The Political Quarterly, 2020
[9] International Journal of Data and Network Science, 2024
[10] sdaia.gov, 2024
[11] insights.onegiantleap.com, 2023
[12] my.gov.sa, 2023
[13] my.gov.sa, 2023
[14] provenrobotics.ai
[15] dga.gov.sa, 2022
[16] mcit.gov.sa, 2023
[17] cst.gov.sa, 2024
[18] socpa.org.sa, 2024
[19] theiia.org, 2023
[20] dgp.sdaia.gov.sa, 2023
[21] National Data Governance Interim Regulations, 2020
[22] socpa.org.sa, 2024
[23] unctad.org, 2021
[24] my.gov.sa, 2024

- Vision 2030 - vision-2030_story-of-transformation.pdf (vision2030.gov.sa).
- SDAIA - PoliciesEn.pdf (sdaia.gov.sa) | and National Data GovernanceInterim Regulations Version 1 June 1st, 2020.
- Navigating NDMO Requirements | BigID.
- Smart Government Strategy in the Kingdom of Saudi Arabia (my.gov.sa) – May, 2023.
- SDAIA - منصة حوكمة البيانات الوطنية (sdaia.gov.sa).
- Privacy Policy in the Kingdom of Saudi Arabia (my.gov.sa) – 28 March 2024.
- Microsoft Word - Personal Data English V2-23April2023- Reviewed-.docx (sdaia.gov.sa) – Personal Data Protection Law, September 2021).
- Emerging Technologies Adoption - Emerging Technologies Adoption (my.gov.sa) – July 2023.
- SOCPA's Auditing Standards Board Approves IAASB's Amendments to ISA No. 600 - SOCPA.
- Saudi Arabi: Leadership of Digital Economy in the Middle East - MCIT_DEC_23_En_V7.pdf - December 2023.
- Saudi Arabia: 3rd Worldwide, a 'Very Advanced' Digital Leader | Digital Government Authority (dga.gov.sa) – October 2023.
- The Future of Technology Risk (isaca.org) – February 2023.
- The top 5 emerging digital technologies in Saudi Arabia (onegiantleap.com) – September 2023.
- Digital Government Authority (dga.gov.sa) - Strategic Directions for Digital Government March 9, 2022.
- Technology and Innovation Report 2021 (unctad.org).
- The Institute of Internal Auditors Signs MoU with New ARABCIIA Regional Body (theiia.org) – February 2023.
- Growing Science (growingscience.com) – International Journal of Data and Network Science, The impact of computer assisted auditing techniques in the audit process: an assessment of performance and effort expectancy - 2024.
- The Changing Role of Internal Auditor as Assurer, Assessor and Advisor (researchgate.net) – 2022.
- Blockchain (cst.gov.sa) – CST.gov.sa, 2024.
- Ai.sa, 2024.

Contacts

Khalid Yasin
Partner, Head of Enterprise Risk Services
E: kyasin@kpmg.com

Mazen Hamad
Partner, Head of Internal Audit
E: mhamad@kpmg.com

Shadi Abuserryeh
Senior Director, Governance, Risk and Compliance
E: sabuserryeh@kpmg.com

Karim El-Mir
Manager, Governance, Risk and Compliance
E: kelmir@kpmg.com

kpmg.com/sa