SNG Grant Thornton

Audit | Tax | Advisory

Business Risk Services

Trends in technology risks - 2024

2024

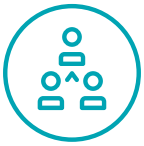
Contents

Trends in technology risks - 2024

With a growing need for technology assurance – from cyber security and transformation programmes to the use of AI, cloud services and third parties – what do Internal Audit and Technology Risk functions need to know to be able to respond to their organisations' key technology risks?

Key technology risk areas for internal auditors and technology risk functions to consider in 2024:

Cyber security



Third-party management

Generative AI

Transformation programmes

Cloud assurance

Embedding security in DevOps

Identity and access management

Technology resilience

IT control programmes and automation

Data management and quality

Cyber security

Cyber security continues to be a critical business risk for the world and South Africa. Some statistics that are mentioned by Accenture noted a 20% increase in incidents others noted an increase in disruption of operational technology.

While data loss and service disruption continue to be two of the major risks associated with a cyber-attack, ransomware attacks are also significant. According to a **2023 Sophos report**, 66% of organisations globally were hit by a ransomware attack in the last year, with the attackers succeeding in encrypting data in **over three-quarters (76%)** of attacks.

What has changed?

Cyber security isn't a new risk. Many organisations already have in-flight cyber security programmes to enhance their controls and their ability to defend, detect, respond, and recover from cyber-attacks. They're also taking proactive approaches to cyber security assurance by implementing continuous monitoring and more advanced threat detection capabilities. Most organisations today have a range of security-focused assurance mechanisms in place, such as obtaining accreditations ***(eg, ISO 27001, Cyber Essentials Plus),*** performing penetration testing, or conducting red-team exercises.

Over the past year we have noted an increasing number of organisations commissioning programmes to further enhance their cyber posture in line with broader and more robust frameworks, such as NIST and CIS. While being well recognised, these frameworks tend to require greater investment to adhere to their requirements. Overall, South African companies are more aware of cyber security.

What should internal audit and technology risk functions do?

- Build a unified picture of the organisation's cyber security assurance processes and shape complementary internal audit plans to build on this existing assurance, reducing duplication.
- Play a key role in providing assurance over cyber security investments and programmes.
- Conduct cyber health checks using established appropriate frameworks, such as NIST or CIS, instead of relying solely on traditional methods like the 10 Steps or Cyber Essentials Plus.
- Assess the arrangements the organisation has in place to defend and respond to a cyber attack, such as ransomware, including the use of immutable backups and processes for responding to attacks.
- Conduct a holistic cyber risk assessment that take the entire organisation into account across the defend, detect, respond, and recover phases.

Third-party management

Organisations choose to use third parties for a variety of reasons to make them more competitive or giving them unique capabilities. By outsourcing certain functions to third parties, organisations can transfer some of the risks associated with those activities to the third party. Third parties may have access to cutting-edge technology or tools that the organisation does not have.

In order to manage risks around service continuity, information privacy, and security, organisations need to have an effective framework of controls in place around third parties.

IT and technology functions are among the largest users of third-party products in the form of third-party tools, SaaS solutions, and direct outsourcing of business activities.

Outsourcing the responsibility for these services, however, doesn't outsource the associated risks, and organisations need to expand their range of assurance activities to cover third-party providers.

What has changed?

The range of third-party providers involved in core business activity is growing. As many organisations reap the benefits of SaaS products and external technical expertise, the operation of the business is increasingly dependent on third parties. This includes many customer-facing services, as well as internal systems (HCM, ERP, etc).

With the increased use of third parties the perimeter of an organisation's cyber defences is effectively increased, consequently the scope of assurance also needs to increase.

Organisations are increasingly establishing in-house capabilities dedicated to marrying skills in both supplier management and security assurance to assess these third parties.

What should internal audit and technology risk functions do?

- Review and help define the methodology for assessing the relative continuity, privacy, and security risk of third-party suppliers– as part of which they should identify the high-risk suppliers (these may not be those with the largest spend).
- Assess the security controls over the most important portion of the supply chain – consider risk vs. reward when assessing other suppliers.
- Ensure procurement functions are involved and control assessments of new suppliers are embedded into the onboarding process.
- Encourage the expansion of supplier assurance activities to include assurance over ending relationships with suppliers (returning / destroying data, severing users access, etc).
- Third Party Management teams should engage with other supply chain risk activities (such as ESG, AML, and modern slavery).
- Conduct a wholistic third party risk management maturity assessment that take the entire organisation into account and identify the areas that require attention.
- Establishing a framework for managing the risks associated with these risks.

Generative AI

The risks associated with generative AI are critical now due to its widespread adoption. Concerns include the potential for biased outputs, security vulnerabilities, and misuse of generated content for malicious purposes. Deep fakes, misinformation, and ethical dilemmas also pose significant challenges. As generative AI becomes integral to various industries, understanding and mitigating these risks is essential to maintain trust, safeguard privacy, and ensure responsible deployment.

Timely attention to these concerns is crucial to prevent unintended consequences, protect against malicious uses, and establish robust frameworks for the ethical and secure implementation of generative AI technologies in an organisation's rapidly evolving digital landscape.

What has changed?

As these technologies rapidly advance and permeate various sectors, the urgency to address and manage these risks has heightened, necessitating swift adaptation of regulatory frameworks, ethical guidelines, and security measures to ensure responsible and safe integration.

Several countries have proposed regulations on how organisations can develop and deploy AI. Failure to adopt these principles could result in reputational damage if your use of AI is perceived negatively, and if confidential information is disclosed due to a breach or other adverse event.

What should internal audit and technology risk functions do?

- Review how the organisation is taking proactive steps to manage the potential risks.
- Test the effectiveness of AI governance controls, with a focus on ethics, security, explain-ability, transparency, accountability, and contestability.
- Use black box auditing techniques and tools to provide assurance over specific AI use cases within the business.
- Stay informed on evolving AI technologies, collaborating with data scientists, and conduct regular risk assessments.
- Invest in employee training on AI risks and incorporate AI-related audits into regular risk management processes to ensure proactive risk mitigation.

Transformation programmes

Organisations are progressing with their change/transformation agendas at full pace, with technology enabled change dominating the portfolio as organisations seek to be more digital both internally and customer facing.

Organisations are adopting and experimenting with leaner and faster approaches to delivering transformation, often labelled as 'agile'.

One of the key programmes of work we are seeing at many organisations is dealing with the challenge of Legacy IT, longstanding or out-of-date infrastructure or applications that are still in use and prevent an organisation from modernising their ways of working and expose them to availability risks and cyber security vulnerabilities.

Research from the CHAOS institute indicted that more than a third of programmes do not achieve its benefits.

What has changed?

Investment into the decommissioning of Legacy IT has picked up as a reduction in risk appetite at the board level for both resilience and cyber security matters has pushed CTOs and CIOs to prioritise keeping the IT estate evergreen.

Agile methodologies vary greatly in maturity mainly based on the level of experience in those running the transformation agenda. The progression to agile methods alongside the more traditional waterfall approach doesn't reduce the need for project assurance. The same broad risks remain, however the identification of controls points becomes increasing difficult.

Additionally, risk events and the overall risk profile of programmes tend to evolve quicker when agile is adopted, therefore assurance approaches need to reflect this.

What should internal audit and technology risk functions do?

- Define a control framework for agile, where delivery teams undertake a comprehensive risk assessment and decide on the Key Risk Indicators (KRIs) to self monitor; which will guide the audit team on how to assure.
- Adopt real-time independent "heartbeat assurance", where auditors attend scrums, sprint meetings, and governance forums to assess controls for decisions to be made.
- Quantify the increased costs of providing resilience and cyber security from running the legacy estate covering the identification, decommissioning, and funding of out-of-date IT BaU costs.
- Ensure new IT solutions are built in sustainable and 'evergreen' ways. Futureproof against Legacy IT, including: ensuring that any IP is owned internally, evergreen provisions are included in contracts with service providers; and use MI to monitor the status and risk mitigation for current and end-of-life software.
- Adopt minimal key controls and governance requirements for all programs.

Cloud assurance

Over the past few years, the use of cloud solutions has increased rapidly. In particular, organisations are increasingly using cloud solutions to host their critical systems, such as ERP and customer-facing applications, or sensitive data, such as personal data, or intellectual property.

Organisations still face challenges around cloud controls and assurance, inconsistent approaches across assurance teams, cloud concentration risks, and lock-in with vendors.

What has changed?

Cloud assurance issues are increasingly being compounded by the inherent complexity of cloud solutions, lack of visibility at all layers of the computing stack, limited understanding of shared responsibilities for managing cloud controls, and varying compliance requirements for companies operating across multiple jurisdictions.

To address these challenges, organisations need to adopt good practices across all three lines of defence and for giving the same amount of attention across all cloud service models (IaaS, SaaS, PaaS, etc). People are key enablers, therefore teams need to upskill around cloud risks and controls, and call on subject matter experts to provide in-depth tailored insight and independent assurance for the chosen cloud solutions.

What should internal audit and technology risk functions do?

- Conduct assessments of cloud environments and controls to provide assurance to senior management and the board of directors.
- Augment teams with cloud subject matter experts who can provide challenge to technology functions on a peer-to-peer level around the design and effectiveness of cloud controls.
- Test the effectiveness of cloud controls and mature assurance activities with increased levels of control testing automation and dashboarding capabilities.
- Review and evaluate third-party vendor risk management processes and controls related to cloud environment.

Embedding security in DevOps

The adoption of DevOps practices is increasing among large corporate organisations, especially in those which internally develop software for business or customer-facing applications. According to Gartner research, 70% of organisations will have adopted DevOps and infrastructure automation by 2025.

Software development risks are exacerbated by the adoption of DevOps, including around insecure configurations and tooling, misalignment of software with business or customer requirements, insufficient documentation, and difficulty in meeting compliance or regulatory requirements. The DevOps industry is currently 'shifting left' on security, which is a deliberate effort to embed security activities earlier in the process.

What has changed?

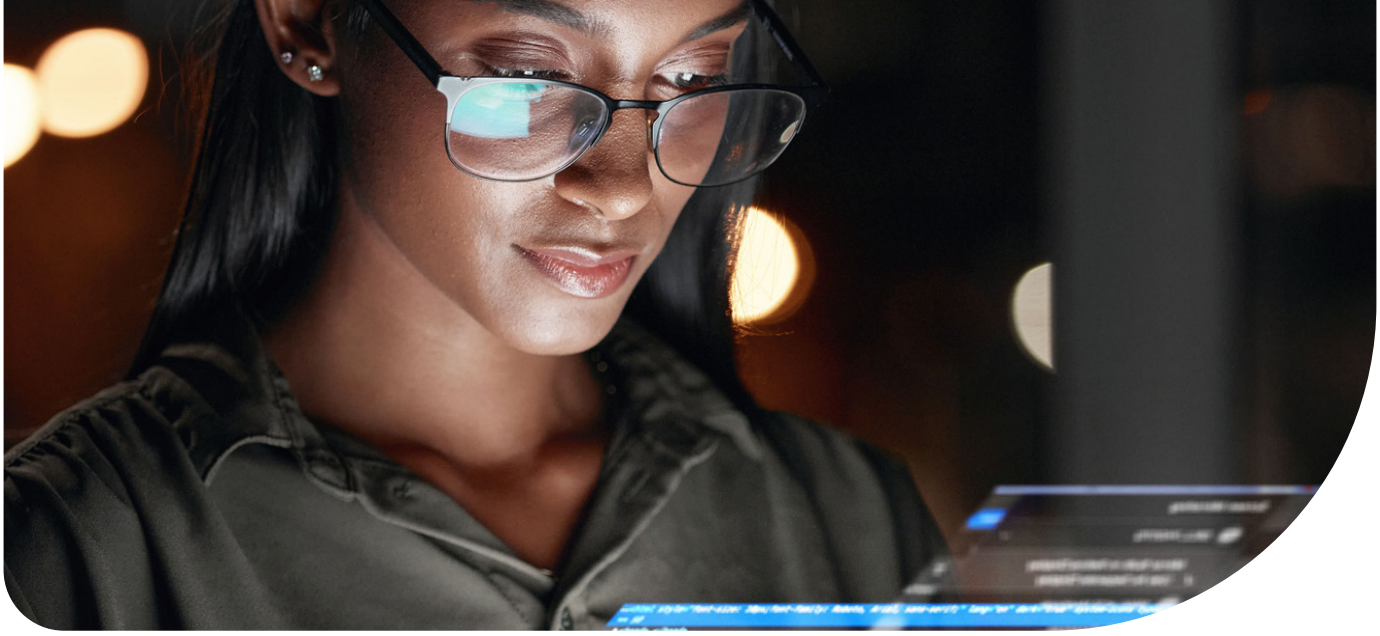
Identity and access management (IAM) is a constantly evolving area with increased threats from 'credential stuffing attacks' (where credentials obtained from a cyber-attack on one system are used to try and breach another systems) and failures of controls at third parties.

IAM can support the requirements of the Code by ensuring:

- users only have access to data and permissions where there is a genuine business need.
- users don't retain access for longer than is required.
- access and changes to key data, and where users perform key transactions, is logged to provide accountability.

What should internal audit and technology risk functions do?

- Regularly assess the risks and controls in place relating to IAM. This should include privileged access, segregating of duty (SoD) risks, and third-party access for vendors.
- Identify bottlenecks in the operation of controls, common failure points and recommend remediations actions to provide appropriate management of the risks.
- Ensure that IAM controls are considered as part of implementing new applications before they are rolled out.
- Invest in technologies to enable the automated and efficient monitoring of IAM controls and SoD conflicts.
- Encourage management to consider implementing technologies to manage federated access if this is not already in place.



Technology resilience

In a technology dependent world, it is often critical that an organisation's IT infrastructure and applications are resilient and continue to operate at acceptable levels during unexpected events or when elements of their technology environment are compromised. When outages occur, businesses need to be able to recover in an efficient and timely manner.

Many organisations are currently facing the challenges of Legacy IT that do not provide the level of resilience they now require. Additionally, the increased adoption of Cloud solutions has expanded the resilience challenge into organisations' supply chains.

What has changed?

The risks of systems outages are not new and have been high on risk agendas for some time. There continues to be, however, multiple high-profile examples of businesses suffering outages due to issues with Legacy IT, human error, natural disasters, cyber-attacks, and control failures at third parties.

The South African context in respect of limited power has already necessitated organisations to step up their resilience programs.

What should internal audit and technology risk functions do?

- Assess the processes for defining the business' resilience requirements, including verifying that the appropriate business stakeholders have been involved.
- Conduct assessments of the resilience of the technology solutions (ie infrastructure and applications) and third-party service providers (including Cloud providers) against the defined business resilience requirements.
- Assess the plans for managing the risk associated with Legacy IT and identify any gaps and residual risks.
- Take part in, as an active observer, or facilitate, tests of resilience arrangements and the related recovery arrangement.
- Ensure that resilience requirements and controls are considered as part of implementing new applications and contracting with new (including Cloud) providers).

IT control programmes and automation

Formulating centralised IT control frameworks can help organisations standardise how IT controls are defined and implemented, ensuring IT controls mitigate the key technology risks their organisation is facing. They also enable control gaps or weaknesses to be easily identified and help facilitate periodic reviews of the control environment.

Automation is crucial as it enhances internal controls' effectiveness, ensures timely compliance, reduces human error, and facilitates real-time monitoring, aligning with regulatory expectations.

What has changed?

IT control frameworks have been a common practice for financial services firms due to regulatory demands. We are seeing, however, a growing number of large businesses from other sectors commissioning programmes to design, implement and test frameworks. With so many businesses running such programmes simultaneously, and with limited resources available in the market, organisations are facing a resourcing challenge, impacting their ability to deliver these.

The need for boards to make sure their organisations have sufficient controls in place, including IT controls. Automation and Robotic Process Automation (RPA) have improved IT control programmes by simplifying repetitive tasks, reducing mistakes, ensuring compliance, and enhancing operational efficiency for companies

What should internal audit and technology risk functions do?

- Evaluate management's identification of the systems that are in scope for completeness of applications, databases, and infrastructure.
- Check whether the framework encompasses all known controls (including application and end user computing controls) based on their understanding of the business.
- Review existing control automation across the organisation and if monitoring is in place that can be leveraged to provide assurance.
- Use automation tools for testing IT controls by applying automated testing scripts, continuous monitoring dashboards, and data analytics to improve efficiency and accuracy in assessments of internal controls.
- Review and track management's action plans to address any control deficiencies or gaps.
- Implement continuous tracking of control improvement activities.

Data management and quality

The risks associated with data management and quality are paramount as they directly impact decision-making, business operations, and regulatory compliance. Poor data quality undermines the integrity of analytics, leading to flawed insights and misguided strategies. Inaccurate or incomplete data poses financial and reputational threats, hindering organisational success.

Robust data management mitigates cyber security risks, safeguarding sensitive information from breaches. Compliance with data protection regulations, such as POPIA, hinges on accurate data handling. Addressing these risks ensures organisations can trust their data, fostering informed decision making, maintaining customer trust, and complying with legal requirements in an increasingly data-driven business landscape.

What should internal audit and technology risk functions do?

- Meet with your CDO or IT/Departmental leads and discuss areas of concern and where data assurance is needed.
- Review the organisation's data strategy and assess if appropriate governance is in place to deliver and monitor its progression.
- Identify gaps in data management compared to good practice and industry frameworks.
- Test the effectiveness of data governance controls, with a focus on policy, standards and quality, oversight, compliance, data architecture, issue management, data culture, data literacy and data asset valuation.

Contact us

Find out how SNG Grant Thornton can help you unlock the potential for growth for your business.

Oupa Mbokodo
Managing Director: Advisory
T +27 (0) 86 117 6782
E Oupa.Mbokodo@sng.gt.com

Maria Pretorius
Director and Head: Business Risk Services
M +27 (0) 83 611 1853
E Maria.Pretorius@sng.gt.com

For general enquiries please contact us at **info@sng.gt.com**

SNG
Grant Thornton