KPMG

Reimagining Internal Audit

Addressing Emerging Technology Risks

KPMG in Qatar

Executive Summary

The role of the internal auditor continues to evolve in the face of dynamic changes to Qatar's technological landscape. All business functions are becoming increasingly dependent on IT systems and infrastructure. The increasing pressure on critical infrastructure has presented internal auditors with new and complex operational and risk management challenges that has disrupted the status quo.

Specifically, internal auditors must consider the following to remain relevant during these times:

- **Keep up with the transformation activities in the country and organization** – Internal auditors must stay aware of and align themselves to the transformation needs across Qatar and the organization. This can be challenging, as it requires the ability to scale up and add relevant and specific technology skills at short notice.
- **Cultivate skills into audit teams that can address new technology and emerging risks** – Internal auditors must keep pace with emerging technology, which can be extremely challenging given the pace of IT change. Being able to call on specific technology subject matter professionals when needed is critical to being effective across the organization.
- **Transform how to work** – Internal auditors must continue to keep pace with ever changing business needs. This may include expanded use of data analytics in audit activity, refining remote working techniques, or adopting more agile approaches to audit execution.
- **Revisit your recruitment plans and sourcing strategies:** The conventional idea of engaging or hiring separate "business auditors" and "IT auditors" has been challenged by the changing business needs. Emerging technology risks have found their way into the conventional audit programs, effectively blurring the lines between IT and non-IT auditors.
- **Rethink how to report findings and make recommendations** – Risk functions are moving toward a quantifiable view of risk to guide the organization's risk and control investments in areas of highest return as well as reducing exposure. Internal audit should follow suit to make their recommendations more impactful to the risk appetite and regulatory / industry requirements.

A challenge Internal Audit functions have always had, and even more so going forward, with a limited budget and resources, is how to best prioritize where your auditors spend their time. Through this report, we have identified key areas where Internal Auditors need to focus to ensure an organization's technology and business interests are protected.

© 2021 KPMG LLC, a limited liability company registered with Qatar Financial Centre Authority (QFCA), State of Qatar and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

01. Cybersecurity

With the concept of hybrid working, we have seen a mass relocation of office workers from corporate networks to studies, living rooms, and kitchen tables. Shortcomings in legacy risk assessments have highlighted the need for enhancements to an organization's cyber security frameworks to effectively manage these widespread events and keep pace with evolving regulatory focus and increasing vulnerability threats.

Organizations should continue to have a laser focus on cyber security, as well as risk and controls frameworks as more business processes are digitized. Based on the elevated risk and increased focus from regulators such as Ministry of Interior (MOI), upcoming National Cybersecurity Agency (NSA), Ministry of Transport and Communication (MoTC), Compliance and Data Protection (CDP), we expect that cyber security will continue to be the number one focus area for Internal Auditors for coming years.

Emerging Risks

Understanding of cyber implications with new workforce model

Given the new hybrid work model, we have seen an increase in cyber fraud. Attackers continue to target the weakest link (usually an uneducated user behind a computer) through phishing , social engineering, spyware, ransomware attacks.

Industry-wide deficiency of cybersecurity skills, within IT and broader workforce

Lack of trained personnel, compounded by decreasing budgets, increases the importance of the implementation of automated tools to focus on cyber risk. In some cases, companies have adequate headcount but are not focused on the highest value-yielding items. Given the changing landscape, this needs to be constantly reevaluated.

What internal auditors need to do?

– **Revise cybersecurity risks and controls**

Internal auditors should review their organization’s cybersecurity risk assessment, processes, and controls, using industry standards and local frameworks (Qatar 2022 Cybersecurity Framework, National Information Assurance Framework) as a guide, and provide recommendations for improvements. Internal auditors should also assess implementation of revised technology security models, such as multilayered defenses, enhanced detection methods and encryption of data leaving the network

– **Cyber awareness / training program**

Internal auditors should review whether cyber awareness programs are embedded in the annual training calendar with a focus on emerging technology risks for employees, subcontractors and vendors. Internal auditors can possibly facilitate the distribution of surveys to gauge awareness of phishing campaigns and assess management’s planned response.

– **Fraud assessment program**

Internal auditors should identify and understand risks to the organization, including weaknesses in controls that present a fraud risk to the organization.

– **Insider threat**

Internal auditors should understand and assess the malicious threat risk coming from inside the organization such as employees, former employees, contractors, or business associates, who have inside information concerning the organization’s security practices, data, and computer systems.

– **Cybersecurity process / cyber cost optimization**

Internal auditors should identify tasks that are manually intensive and time consuming to explore whether automation can be leveraged. This allows professionals to focus on strategic tasks and reduce the repetitive aspects of collecting, analyzing, and reporting data related to threat activity.

© 2021 KPMG LLC, a limited liability company registered with Qatar Financial Centre Authority (QFCA), State of Qatar and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

02. Cloud Security

Organizations continue to invest in technology to achieve cost reduction, process improvement and efficiency. Cloud solutions, for example, are replacing the traditional use of data centers as organizations are looking towards reduced risk of non-compliance, increased security, greater resiliency and scalability. At the same time, the role and requirements of security are changing as organizations embark on their cloud journey.

Emerging Risks

Absence of appropriate cloud governance controls and improper management of third-party risks may lead to exposure of sensitive data with unauthorized personnel.

What internal auditors need to do?

— **Cloud strategy and framework**

Internal auditors should assess the organization's cloud strategy, including the physical location of data, as well as broader operational and compliance risks to demonstrate adherence with circulars from MOI, upcoming NSA, MoTC, CDP and Qatar Central Bank. Internal auditors should have a good understanding of the organization's cloud strategy and the cloud roadmap to facilitate the development of a multiyear, risk-based audit plan based on the cloud roadmap.

— **Cloud adoption, onboarding, and implementation**

Internal auditors should assess the organization's process for identifying, adopting, and implementing cloud solutions and work side by side with the business as it embarks on the transformation. This close collaboration can be achieved in the form of a pre-implementation/real-time implementation program audit, in which Internal Audit is involved in every step of the transformation, from planning to execution and delivery. Internal auditors can provide management with critical insights and considerations on a real-time basis, including providing controls and security integration workstream support.

— **Cloud security**

Internal auditors should periodically assess and perform controls validation to provide ongoing monitoring across cloud infrastructure, data, and application layers. At a strategic program level, Internal Auditors must have a seat at the table as part of the cloud steering or governance committees. While retaining independence is crucial, internal auditors can provide valuable advice to help business leaders understand the risk and regulatory considerations stemming from cloud deployments.

– **Data ownership and management**

With the rolling out of a strong regulatory framework around data management within Qatar, it is imperative upon internal auditors to assess the risks of unauthorized access over their business data. Generally, the risk of unregulated access over production data goes unchecked in a SaaS environment, as the privileged access is retained with the cloud service providers. Internal auditors should re-visit their agreements with their cloud service providers and request either a SOC 2 report or exercise their 'right to audit' clause to ensure their business data is adequately protected.

© 2021 KPMG LLC, a limited liability company registered with Qatar Financial Centre Authority (QFCA), State of Qatar and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

03. Third Party Risks

The changing business and technology landscape is placing added pressure on third party framework across the organizations. While third parties are vital for an organization to prosper, they can also expose it to immense risks. Third-party risk management (TPRM) framework addresses the risks presented by third parties including supply chain disruption, reputational damages, corporate fines, and cyber breaches. Attestation reports such as SOC 1, SOC 2, SOC for cybersecurity and SOC for supply chain management are few powerful tools used internationally to gain comfort the control environment of third party suppliers.

Emerging Risks

Organizations are increasingly relying on third party suppliers to deliver business-critical products and services to their clients and customers. Unfortunately, they are finding that failures by third parties can rapidly tarnish their reputations and have significant downstream operational and cost implications. As organizations address their concerns about these issues, they need a clear strategy for the selection, approval, and management of third parties. As there are a myriad of stakeholders involved, from the business as well as the procurement and risk- oversight functions, developing and implementing this strategy continues to be highly challenging.

What internal auditors need to do?

— **Third party lifecycle management**

Internal auditors should assess how the organization can consistently and holistically identify, monitor, and manage the third party risks, specifically risks around remote contingent workers and third party services. Internal auditors can conduct an independent review of organization’s third party risk management program to assess the processes and controls over the third party lifecycle, including third party selection, contract negotiation, ongoing monitoring of risk and performance, and termination.

— **Third-Party risk assessment**

Internal auditors should assess management’s evaluation of the risk that arises from working with vendors. A review of the IT vendor risk assessment would include reviewing management’s documentation about the risk of third parties (e.g., geography, services, contracting), concentration risk and initial risk ranking of third parties, review of third party questionnaires and results, vendor due diligence results, and any IT risk acceptances.

— **IT Third-Party cyber resiliency**

Internal auditors should assess and understand the cyber resiliency of critical IT vendors and provide assurance to management about their third- party vendors’ capacity to mitigate against large-scale disruptive events, cyber-resiliency preparedness, recovery capability and capacity, oversight of subcontractors, Recovery Point Objective (RPO) and Recovery Time Objective (RTO), data confidentiality agreements, oversight of fourth parties, and cyber insurance.

— **Contract compliance program**

Internal auditors should review the organization’s contract compliance program to assess management’s oversight of vendor performance. This involves a review of management’s analysis of contractual obligations with third parties, IT security considerations, performance metrics, business and infrastructure changes at the vendor, cybersecurity incidents, outages, non-availability of services, review of penetration test results, SOC reports, and regulatory compliance.

© 2021 KPMG LLC, a limited liability company registered with Qatar Financial Centre Authority (QFCA), State of Qatar and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

04. Data Privacy

Organizations recognize data as an asset that increasingly needs protection via robust data governance and controls across their organization and through their third parties. Continued data security breaches and data sharing incidents are influencing public and regulatory expectations for increasingly stringent data privacy and security requirements ensuring public policy and enforcement will continue at the local, national and global levels. Organizations must assess compliance to legally binding regulation for protecting personally identifiable information as per the PDPPL[1] and EU GDPR[2]. Entities must implement processes, controls and technologies required to build a sustainable data privacy capability that is aligned to the business and is focused on compliance to general principles of data privacy.

Emerging Risks

The bar for data privacy and protection of personal data[3] is set by regulatory environment of the industry and the views of the board of directors. Data has now become an enterprise-wide priority, compounded by industry-agnostic legislation that is sure to impact several organizations across Qatar, which store, process and / or transfer personal information of individuals or entities. Intellectual property loss, legal expenses, property loss, reputational loss, and time loss, as well as administrative costs are few of the emerging risks which require immediate attention by internal auditors.

What internal auditors need to do?

– **Enterprise-wide privacy program**

Internal auditors should assess the organization’s process to plan for regulatory changes and perform a comprehensive review of the enterprise-wide data privacy program in line with PDPPL. Evaluating the scope and effectiveness of the privacy program, including the established governance processes, roles and responsibilities, training, and risk management can provide a point of view on how equipped the company is to the compliance requirements of PDPPL and EU GDPR and effectively sustain compliance on an ongoing basis.

– **Data management and governance audit**

Privacy must be an integral component of the business model with the goal of creating a sustainable and effective data-protection strategy. Companies should assess data-management/data-governance processes, as well as the adoption of these processes by business units. New accounting standards will require companies to strengthen their data-gathering process and data-governance procedures. Internal Auditors can perform comprehensive data governance and data management audits to help ensure all data used is consistent, accurate, complete, and secure. As part of the review, Internal Auditors can review overall data governance, data dictionary and lineage, data quality, metadata, master data management, and data classification. This would also include an assessment of the data domain roles, data change management, data handling and processing, information architecture, data lineage, metadata management, data quality rules, and data classification.

[1] PDPPL: Personal Data Privacy Protection Law, 2016
[2] EU GDPR: European Union General Data Protection Regulation, 2016
[3] Personal Data: Data of an individual whose identity is defined or can be reasonably defined whether through such Personal Data or through the combination of such data with any other data (Law No.13 of 2016).

© 2021 KPMG LLC, a limited liability company registered with Qatar Financial Centre Authority (QFCA), State of Qatar and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

05. Identity and Access Management

The concept of Identity and Access Management (IAM) is critical to ensure appropriate protection of your data and applications and limit any unintended access or actions. IAM addresses the mission-critical need to ensure appropriate access to physical and logical assets and associated facilities are limited to authorized users, processes, and devices. Access is granted as per the roles and responsibilities of the users based on the principal of least privilege and segregation of duties is enforced.

Emerging Risks

Identity and Access Management (IAM) should be an integrated component of design of the control environment, especially with the increased use of cloud technologies and bots, which increase the complexity of authentication and authorization. Compromised passwords are often the source of identity theft and may result in compromise of corporate network assets. Companies need to assess at what point it makes sense to employ more advanced authentication methods (touch/face ID/voice) to replace passwords.

What internal auditors need to do?

– **IAM governance program**

Internal auditors should assess management's overall IAM governance program, assess IAM policies and procedures, access lifecycle management, access control, asset management, and procedures in place for monitoring and logging of access/activity.

– **Privileged access**

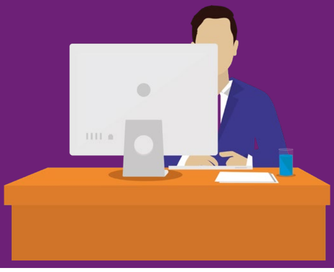
Internal auditors should assess management's controls over privileged access, with a focus on management's definition of privileged access at all layers (application, devices, and supporting infrastructure), classification of accounts, account lifecycle management controls (request, addition, change, deletion), and controls over the scope and use of service accounts.

– **IAM implementation readiness assessment**

Depending on the organization's maturity level, internal auditors can support management's discussions about developing a holistic IAM program. This could involve an assessment of the organization's needs (roles definition, access requirements, etc.) and identify gaps between those needs and management's IAM program, including the creation of policies and selection of tools.

© 2021 KPMG LLC, a limited liability company registered with Qatar Financial Centre Authority (QFCA), State of Qatar and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

06. Hybrid working model



With the hybrid working model being implemented across the globe and within Qatar, it is more critical than ever to be aware of more pressing risks related to working from outside the corporate network and security of office premises.

Internal Auditors should focus on the threats from implementation of new technologies, and the changing landscape of emerging risks.

Emerging Risks

It is now widely accepted for organizations to reduce their overhead costs by decreasing burden on office facilities and allowing the employees to work from home on a hybrid working model. Supporters of this model would argue that productivity of work force has increased, but the fact remains that this operating model has introduced new risks which need to be addressed by Internal Auditors. As employees continue to work from outside the security of the corporate network and office premises, the risk of unauthorized exposure of confidential data needs to be addressed.

What internal auditors need to do?

– **Assess the scalability and capacity of remote IT service management**

If a remote working environment continues to be in place longer term or for the indefinite future, the process followed by IT service management and the capacity of IT service management to assist with end-user issues related to an “at home” IT environment should be reviewed. We have seen IT service management functions overwhelmed with new requests from end users to support issues related to accessing critical corporate applications, home printers, home Wi-Fi connectivity, etc.

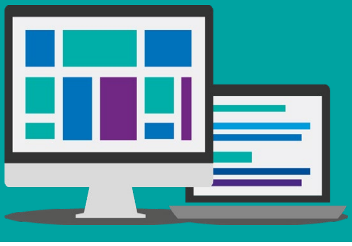
– **Assess technology implications of return-to-office framework/strategies**

Internal Auditors should assess how IT environment has been impacted and where risk assessment framework has been updated to reflect the changes. Some areas to consider:

- Does threat assessment/risk remain the same or should it be adjusted?
- What updates are needed to the Business Continuity Planning/Disaster Recovery Planning plan?
- Will the target operating model (TOM) change if a portion of IT professionals are remote, and some are physically in the office?
- What is the level of IT involvement in the return-to- office steering committee?

© 2021 KPMG LLC, a limited liability company registered with Qatar Financial Centre Authority (QFCA), State of Qatar and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

07. DevOps/Agile



Modern practices in software development, such as DevOps, require that the functions of auditors evolve accordingly. Rather than building plans based on last year's performance and risk assessments, including Internal Auditors within DevOps enables companies to guard against inefficiencies. When controls are designed and implemented correctly in DevOps, it enables the organization to address the end-to-end traceability of the change.

Emerging Risks

Organizations are challenged to deliver high-quality code fast, often, and securely. The need to innovate and deliver at scale is becoming an expectation of agility, not an exception.

What internal auditors need to do?

– **Evaluate DevOps strategy, governance, and training**

Internal auditors should evaluate the DevOps strategy by focusing on governance, adoption of DevOps practices, production management, DevOps capabilities, and training/development. Internal Auditors should assess the overall governance and strategy around DevOps.

– **Assess integration of security in the DevOps process**

Internal auditors should also assist management in identifying opportunities to increase security through an evaluation of controls, behaviors, or capabilities across the software development life cycle (SDLC) for risk reduction. This can be achieved through "light-touch" security testing across the organization's most critical applications, which could then translate to more detailed security requirements to provide to developers at project initiation.

– **Assess possible segregation of duties (SOD) concerns and mitigation**

Internal auditors should perform a deep dive on change management covering access controls and segregation of duties (SOD) to identify gaps brought by developers' access to production.

– **Review key tools supporting the CI/CD process**

Internal auditors should conduct a review to understand critical process and tools supporting the CI/CD and DevOps processes. For identified critical processes/tools, Internal Auditors can perform a process review to identify gaps and key controls unique to CI/CD automation and tools.

© 2021 KPMG LLC, a limited liability company registered with Qatar Financial Centre Authority (QFCA), State of Qatar and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

08. Operational Resilience

Operational Resilience takes an outcomes-based approach that changes the traditional, asset-focused business continuity plan from a periodic exercise to an asset for long-term organizational resilience and growth. In the war to win the trust of customers and other key stakeholders, organizational resilience is a must-have pillar of strength these days

Emerging Risks

Whether on premises or in the cloud, IT resiliency is the ability to adapt to planned or unplanned events while keeping services and operations running continuously. When the highest IT resiliency is implemented, data remains available, IT infrastructure stays operational, disruptions are minimized, and service levels are restored quickly. This is accelerated through the widespread adoption of cloud technologies.

What internal auditors need to do?

– **Assess investment process for updating legacy systems and infrastructure**

Internal auditors should assess how the organization prioritizes investment decisions for modernizing legacy systems and strengthening technology infrastructure.

– **Assess dependencies between internal and third parties**

Internal auditors should assess how dependencies between internal and Third-Party systems are mapped, analyzed, and tested to validate the feasibility of stated recovery time objectives and achieve resumption of end-to-end business services. This would also include a review of penalties for third parties that fail to deliver services and ensure there are exit strategies for each vendor.

– **Review communication plans**

Internal Auditors should review communication and crisis management plans to ensure they provide timely information to, and manage the expectations of, customers, market participants, and regulators following a disruptive event.

– **Disaster recovery system architecture design assessment**

Internal auditors should review the current state of disaster recovery architecture for IT network, systems, and applications to identify any gaps in the ability of IT disaster recovery to meet stated business requirements (e.g., identification of technical single points of failure and assessment of recovery times versus business needs).

– **Ransomware resilience**

Internal auditors should assess both proactive and reactive capabilities and respective processes to recover from a ransomware attack. This should include a review of the process to identify, contain, and recover impacted systems compromised by the attack. Internal Auditors should assess management's identification of systems that are most vulnerable to ransomware attack, including Third-Party managed systems and risk mitigation/controls, to help prevent and/or limit the impact of a ransomware attack.

– **Business impact assessment regarding loss of site and loss of key technology scenarios**

Internal Auditors should consider and report on the ability of IT disaster recovery capabilities to meet business requirements given a range of agreed-to disruption scenarios including but not limited to loss of key site(s) housing technology equipment/services, loss of key Third-Party IT service providers, loss of key IT service personnel.

© 2021 KPMG LLC, a limited liability company registered with Qatar Financial Centre Authority (QFCA), State of Qatar and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

How can we help?

Internal Audit function is indeed a strategic arm of the business. We believe that internal auditors could provide tangible value to business by focusing on emerging technology risks and providing practical recommendations that assist in achieving business objectives, in addition to validating compliance and providing overall risk coverage.

KPMG's approach reflects direct input from our experience in dealing with regulators, industry experts, senior management and audit committee chairs, who report a gap between their expectations and what Internal Auditors are delivering.

KPMG helps Internal Audit function take a strategic approach, elevating the function in terms of the insights, results and demonstrable value it can provide the organization. Bringing industry knowledge and experience to Internal Audit function is critical to our value proposition and to helping you provide strategic value and insight relevant to the unique environment and context of life sciences.

About our Technology Risk Services

KPMG can support your Internal Audit function with a range of services including, but not limited to:

- Outsourcing and co-sourcing Internal Audit function
- Review of General IT Controls and Business Automated Controls
- Data Analytics (D&A) enabled Internal Audits
- Cybersecurity reviews (NIST, Qatar 2022 Cybersecurity Framework, SWIFT CSP)
- National Information Assurance (NIA) compliance audits
- IT Attestation (SOC1, SOC2, SOC for Cybersecurity)
- Review and implementation of Data privacy framework
- Review of ERP security controls
- Enterprise IT risk management
- IT governance assessments
- IT Projects Reviews

Contact us

Ali Al-Shabibi
Partner
KPMG in Qatar
M: +974 7471 2768
E: aalshabibi@kpmg.com

Suleiman Gammoh
Manager
KPMG in Qatar
M: +974 6625 3672
E: suleimangammoh@kpmg.com

Idrak Ahmad Khan
Assistant Manager
KPMG in Qatar
M: +974 3342 7638
E: idrakk@kpmg.com

© 2021 KPMG LLC, a limited liability company registered with Qatar Financial Centre Authority (QFCA), State of Qatar and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.