Governance, Risk, and Control

Part 3: How Digital Transformation Is Transforming GRC.

- **The scope of digital transformation.**

The COVID-19 pandemic accelerated the digital transformation trend, and it continues to progress rapidly. Organisations are driven to embrace digital transformation to increase profits and efficiency and keep up with emerging risks, such as inflation, geopolitical tensions, economic uncertainty, supply chain disruptions, and ESG-related regulation changes.

A recent Gartner report reveals that 89% of board directors now consider digital business as an integral part of their growth strategies. However, only 35% claim to have achieved or be on track to achieve their digital transformation goals.

According to Jorge Lopez from Gartner, technology used solely for operational excellence is insufficient to achieve the strategic benefits that boards are seeking from digital investments.

Digital transformation varies depending on the location, industry, and organisation, and there is no one-size-fits-all approach. However, successful digital transformation involves more than just implementing technology; it requires a shift in mindset that allows organisations to reimagine their business models and processes to leverage the opportunities created by emerging technologies.

In a world of constant disruption, future-savvy boards and leaders view upheavals and risks as potential opportunities for growth. As technology continues to play an increasingly significant role in driving business success, CEOs and CIOs must adopt this forward-thinking mindset.

- **Digital transformation's effect on GRC.**

The impact of digital transformation on GRC functions has been significant, leading to challenges in maintaining adequate levels of coverage.

With the emergence of systems like ChatGPT and Bing Chat, organisations need to act quickly as employees are already using these technologies for various tasks. Some organisations may block them entirely, while others with better technology understanding will create internal guidelines for their usage.

Developing strategies and guidelines will involve various parties, including the chief digital and information officer, IT and risk management teams, legal, and finance groups. However, effective communication and enforcement of these guidelines are equally critical. Companies can operate on an honour system to some extent, but more formal measures, such as browser banners reminding employees of the guidelines, are necessary.

To seamlessly manage these emerging technologies, an agile and adaptable GRC function should be in place before they enter the organisation's risk landscape. However, not every organisation may have the foresight or resources to do so. To succeed in this new era, internal audit needs to take initiatives in various ways and be prepared for the challenges brought by such technologies.

Governance, Risk, and Control

- **Keeping a seat at the table.**

Internal audit plays a crucial role in supporting effective GRC, particularly in organisations lagging in updating their GRC functions. To pursue meaningful changes, investments are necessary, but obtaining buy-in from all levels of the organisation can be challenging. Internal audit, with its position at the table, can relay the benefits of digital transformation and ensure informed decisions are made by management and the board.

Maintaining a seat at the table is essential for internal auditors to fulfil their mandate effectively. By engaging in regular and informed communication with stakeholders, internal audit fosters a strong organisational culture focused on risk assurance and compliance. Leveraging communication channels to their full potential ensures that GRC remains a top priority for the organisation.

- **The risk of GRC tool proliferation.**

Not all controls available for implementation may contribute to a successful GRC-focused culture.

The digitalisation of organisational processes has led to the availability of numerous data analytics tools with GRC modules as add-ons. However, if individual GRC functions adopt separate tools, it can hinder internal audit from presenting a comprehensive view of GRC to stakeholders.

Using multiple SaaS tools with GRC components can lead to fragmented risk assessments and difficulties in managing the overall GRC approach. To address this risk, one strategy is for GRC stakeholders to assign individual process owners to streamline the GRC approach and establish clear communication with internal audit, ensuring a cohesive and reportable GRC process. Collaboration and integration are essential to achieve effective GRC practices in such a complex technological landscape.

The push for managing overall risk is commendable, but discussions about the division of duties and alignment of priorities and scopes are necessary. There should be a balance between shared responsibility and top-down control in GRC practices.

Internal audit should let stakeholders drive GRC objectives and processes while promoting collaboration and transparency. Being part of the conversation allows internal audit to raise red flags when necessary. Understanding broader objectives and responsibilities enables adequate oversight without unnecessary interference in individual roles.

- **Strategies to lead and promote discussion.**

Internal audit should lead by example in promoting the benefits of digital transformation by showcasing the effectiveness of its function. While some aspects of digital transformation may require significant budgets, basic automation using readily available tools like Excel, Power BI, and other Microsoft productivity tools can be implemented at minimal cost.

Governance, Risk, and Control

Internal audit can also contribute by sharing knowledge and identifying critical competencies lacking in GRC functions. By highlighting gaps in workforce knowledge and promoting corrective measures, such as communal training, hiring external parties for upskilling, or incorporating skills-based training into job roles through online resources, internal audit can play a constructive role in advancing digital transformation across the organisation.

Organisations can promote upskilling in-house by encouraging interactions and collaborations with other departments. One strategy is to create a website where employees can share innovation ideas, vote, and comment on them in a controlled manner to build competencies collectively.

Informal discussions through platforms like communal chats or Slack channels can also foster knowledge-sharing and partnerships. Internal audit can become a valuable part of these discussions by acquiring knowledge about emerging technologies relevant to GRC.

Having a significant degree of knowledge allows internal audit to meaningfully engage stakeholders in discussions about technologies like AI and data analytics. By being curious, open-minded, and continuously learning, internal audit can play a role in shaping digital transformation in GRC and even provide consultation on areas such as AI implementation in compliance.

- **Be an active part of the internal audit community.**

In summary, digital transformation is irreversible, and organisations must either embrace it or risk falling behind. This sentiment should be embraced at all levels of the organisation, from the C-suite to GRC, operations, and internal audit. In today's interconnected world, it is essential to extend efforts beyond the organisation's boundaries and actively participate in global audit discussions.

Engaging with local IIA chapters, attending webinars, and conferences can foster valuable connections and learning opportunities. The best learning often comes from hearing the experiences of others, and maintaining industry connections is crucial in a rapidly changing profession. While technology continues to advance, genuine human connection remains indispensable for professional growth and success in navigating constant change.

What should Internal Auditors do?

Standard 1210 - Proficiency and Due Professional Care

Internal auditors are required to possess the necessary knowledge, skills, and competencies to effectively carry out their responsibilities. Embracing digital transformation requires auditors to stay current with emerging technologies, data analytics tools, and automation techniques. By demonstrating proficiency in these areas, internal auditors can lead by example and showcase the benefits of digital transformation.

Internal audit can play a constructive role in advancing digital transformation across the organisation by actively sharing knowledge and identifying critical competencies that may be lacking in GRC functions.

By highlighting areas where workforce knowledge gaps exist, internal auditors can promote corrective measures, such as offering communal training sessions, engaging external experts for upskilling, or integrating skills-based training into job roles through accessible online resources.

Governance, Risk, and Control

This collaborative approach fosters a culture of continuous learning and development, contributing to the organisation's successful digital transformation journey.

Reference:

https://www.theiia.org/en/content/articles/global-knowledge-brief/2023/june/grc-part-3-how-digital-transformation-is-transforming-grc/

Tone at the Top

TONE at the TOP®

Providing senior management, boards of directors, and audit committees with concise information on governance-related topics.

Issue 117 | June 2023

Providing senior management, boards of directors, and audit committees with concise information on governance-related topics

- **AI: The Governance Imperatives.**

The modern advancements in AI, such as machine learning and predictive analytics, offer enticing business opportunities. With improved computing power, affordable data storage, and remote access to applications, AI is becoming more accessible to organisations. However, there is a risk that boards may view AI as solely an IT concern, overlooking its pervasive impact and governance implications. AI should be recognised as a board-level concern, understanding its potential influence on various aspects of the organisation.

Technologies like AI have the potential to profoundly transform business operations, as demonstrated by products like ChatGPT. As businesses explore AI adoption, leaders should carefully consider its impact on workplace culture, emerging regulations, and the broader legal, ethical, and moral implications of its use. Given the numerous governance considerations associated with AI, it should be a priority topic on directors' agendas, as its exponential disruptive capabilities make it a board-level issue.

- **Key Considerations.**

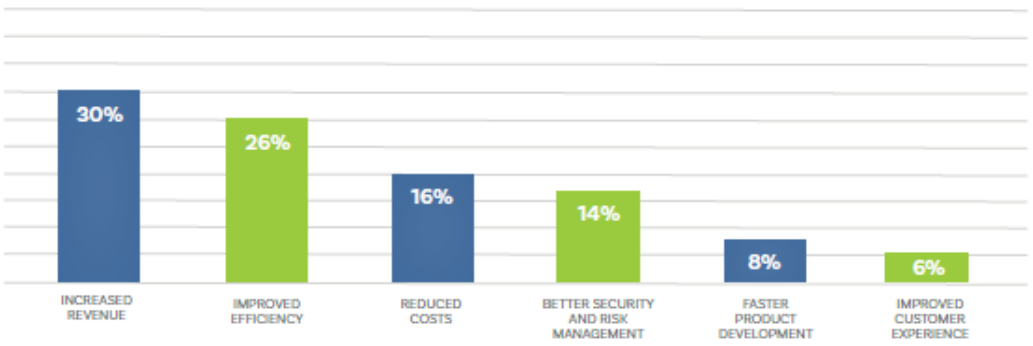
Here's a look at some of the questions board members should be asking in their AI governance role, and the ways that internal audit can help them develop answers. Issues for boards include:

- **What does AI encompass?**

AI encompasses various applications like natural language processing, expert systems, and machine learning, enabling it to process vast volumes of data and simulate human intelligence. It is prevalent in everyday life, from autocorrect features to smart speaker responses. In business, AI is used in medical diagnostics, supply chain optimisation, and process automation. Future uses include faster clinical trials, AI-driven micro-fulfilment centres, and improved product design.

AI's capabilities also extend to content creation, translation, and the development of various products, showcasing its versatility and transformative potential across industries.

Figure 1 - **By 2025, what likely tangible benefits might AI provide?**



Tone at the Top

What risks do AI applications pose?

AI can pose threats on many levels. Indeed, given the uncertainty around AI, more than 1,000 tech leaders, researchers, and others recently called for a pause in the development of the most advanced AI systems, pointing to "profound risks to society and humanity.

- Employment concerns.

A significant social consideration in the context of AI. Economists from Goldman Sachs estimate that generative artificial intelligence, like ChatGPT, could automate up to 300 million jobs worldwide, potentially computerising 18% of work globally. This raises questions about the impact of AI on the job market and the need for adaptation and reskilling in the face of automation.

- Imperfect technology.

AI still has limitations, as evident in early experiments with driverless cars and other applications. Unlike humans, AI lacks context and judgment in analysing information. Machine-learning tools may inherit biases, leading to unintended consequences, such as exclusion in recruiting or omitted valuable data. AI in 2023 remains prone to biases like its human counterparts. Misunderstood spoken language and AI "hallucinations" producing false information are concerns. These limitations can result in incorrect responses, erroneous data spreading, and potential liability concerns, undermining processes and confidence in the organisation's technology.

- Privacy

AI can help mitigate cybercrime; it also raises privacy risks due to the collection of personal data. Security professionals express the need to reassure customers about data usage in AI. Privacy policies may require updates to address AI-related challenges and provide reassurance to stakeholders. Directors should consider legal questions regarding board oversight of AI-powered technology to ensure compliance and responsible use.

- Missed opportunities.

Companies may lack the necessary resources and specialised expertise to fully utilise AI tools effectively. Access to large datasets for AI learning and improvement may also present challenges for some businesses. To harness the potential of AI, companies must address resource constraints and ensure access to the required data for optimal AI performance.

How Can Internal Audit Contribute to AI Governance?

Internal audit plays a crucial role in providing boards with a comprehensive understanding of an organisation's risks and the impact of AI throughout the company. Boards can rely on internal audit for unbiased assessments of AI controls' appropriateness, effective implementation, and governance monitoring.

Internal audit offers assurance that AI usage aligns with the organisation's governance principles, covering accountability, transparency, robustness, fairness, inclusivity, privacy, security, and safety.

"A well-trained internal audit function that is well-versed in AI will be an invaluable asset to any board," according to Julio Tirado, CIA, director of internal audit at Spirit Bank. He identified three roles for internal audit in this evolving risk area.

Tone at the Top

• Consultant. By collaborating with management in the design phase of any AI systems, internal auditors can offer a pre-emptive evaluation of risks, making it possible for the organisation to build a safe and secure system. "When companies bring in internal audit on a consultative basis, they can spend more time on the business and less time putting out fires," Tirado said.

• Assurance. Internal audit can research and identify risks that can have an impact on crucial considerations such as privacy, security, compliance, and third-party risk management, the last of which may be a key challenge with AI, Tirado said. "We can add unique value in our traditional role of performing audit procedures that identify risks."

• Idea leadership. Internal audit can use its global view of the company to take a leadership role in understanding AI's impact on the current environment as well as emerging challenges and opportunities. For example, internal audit can brief the board and the audit committee on the use of tools such as ChatGPT not only in audit but also from the perspective of managers in various functions, Tirado noted.

Failure to make use of internal audit as a resource in addressing AI carries its own risks, Tirado said, including:

• Inadequate identification of risks, controls, and potential process improvements.

• Non-compliance with relevant rules, regulations, and policies, including potential regulation of AI.

• Missed opportunities to enhance stakeholder confidence—including shareholders and regulators—with independent and objective assurance on AI issues.

What should Internal Auditors do?

Standard 1110: Organisational Independence

Internal audit collaborates with management during the design phase of AI systems, fulfilling a consultative role. To maintain organisational independence, internal auditors must ensure that they remain objective and impartial during the evaluation. They should not be unduly influenced by management, or any other parties involved in the AI system's development.

Internal audit's role in providing assurance that AI usage aligns with the organisation's governance principles, including accountability, transparency, and privacy, falls under the context of organisational independence to deliver unbiased assessments, internal auditors must maintain independence from the areas they audit, including AI initiatives.

Internal audit taking a leadership role in understanding AI's impact and briefing the board and audit committee aligns with organisational independence. By maintaining independence, internal auditors can objectively communicate insights and potential challenges without being influenced by management biases or pressure.

By adhering to this standard, internal audit can fulfil its roles effectively and be a valuable asset to the organisation in managing AI risks and aligning AI usage with governance principles.

Reference:

https://www.theiia.org/en/content/articles/tone-at-the-top/2023/tone-at-the-top-ai-the-governance-imperatives/

White Paper on Shariah Audit

Shariah Audit: Definition, Process and Scope

Shariah audit practices in Malaysia originated within Islamic financial institutions' internal audit function. The definition of Shariah audit, based on the Institute of Internal Auditors' International Professional Practices Framework, involves an independent assessment of internal controls, risk management systems, governance processes, and overall compliance with Shariah principles in Islamic financial institutions. Shariah audit serves as the last line of defence to ensure Shariah compliance, complementing the three lines of defence principle used across various industries and situations, which includes management, risk and compliance, and audit functions. Shariah auditors face the challenge of integrating Shariah compliance within the existing auditing framework, requiring versatility and agility to suit the diverse activities and regulations of different sectors.

- **Shariah Audit Process and Scope.**

The Shariah audit function in Islamic financial institutions aligns with existing internal auditing practices but incorporates Shariah elements present in their products and operations. Effective Shariah audit requires a combination of accounting, auditing, and Shariah knowledge. The scope covers internal control, risk management, and governance aspects of operations in accordance with Shariah principles.

Minimum requirements for a Shariah audit function include establishing an audit methodology, generating an audit plan, creating documented audit programs, and communicating results through an audit report to the board and Shariah committee. The report includes findings, rectification recommendations, and the auditee's responses and action plans.

A risk-based Shariah audit (RBSA) approach is emphasised, focusing on areas with significant Shariah non-compliance risk to optimise audit time and resources and provide a valuable final Shariah audit report with risk implications tied to findings.

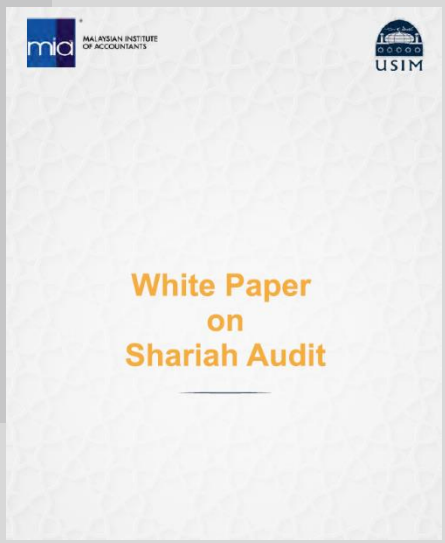
- **Issues and Challenges in Shariah Governance.**

Shariah audits in Malaysian Islamic financial institutions serve two main purposes: compliance with the Islamic Financial Services Act (IFSA) of 2013 and to prevent financial losses and reputational impacts due to Shariah non-compliance. Widespread Shariah audit practices are urgently needed, presenting a challenge and opportunity for auditors to develop integrated auditing and Shariah competencies.

Market players advocate for a holistic Shariah audit approach aligning with Maqasid al-Shariah's broader objectives. This goes beyond compliance with Shariah contracts and extends to areas like income determination, ESG reporting, zakat calculation, and implementation of Values-Based Intermediation (VBI).

Roundtable discussions with Shariah auditors, Chief Internal Auditors, and Shariah officers reveal pressing issues and challenges in the Shariah audit landscape across various sectors, including Islamic banking, takaful, Islamic capital market, Public Trust Entities, Islamic co-operatives, ar-rahnu, and State Islamic Religious Councils.

White Paper on Shariah Audit



Islamic Banking and Takaful.

Islamic financial institutions (IFIs) currently embed Shariah audit within their operational and risk-based audit coverage, as there is no specific Shariah audit framework issued by regulators. Instead, they rely on existing International Internal Auditing (IIA) standards to guide their auditing processes. This practice is consistent with the findings of a previous study indicating that most IFIs use conventional auditing methods due to the absence of a Shariah auditing approach.

Shariah auditors in IFIs should possess experience in business and control functions like Compliance, Shariah Compliance Review, and Risk Management. Having a comprehensive understanding of these areas enables auditors to effectively detect failure points related to Shariah compliance.

Respondents emphasise the need for Shariah auditors to have multiple competencies. They should be well-versed in various Shariah issues and regulations that impact IFIs' financial statements and operations. Formalising Shariah rules and frameworks and having talented individuals with adequate skills and knowledge in both Shariah and accounting disciplines are crucial for elevating Shariah compliance within the industry. Competent auditors will play a pivotal role in driving the implementation of Shariah compliance within Islamic financial institutions.

Islamic Capital Market.

The Islamic capital market sector faces three key issues concerning Shariah governance and assurance:

- Inadequate knowledge of operational Shariah issues by frontliners.
- Insufficient number of internal auditors well-versed in the Islamic capital market and Islamic fund management.
- Lack of talent for the appointment of Compliance Officers.

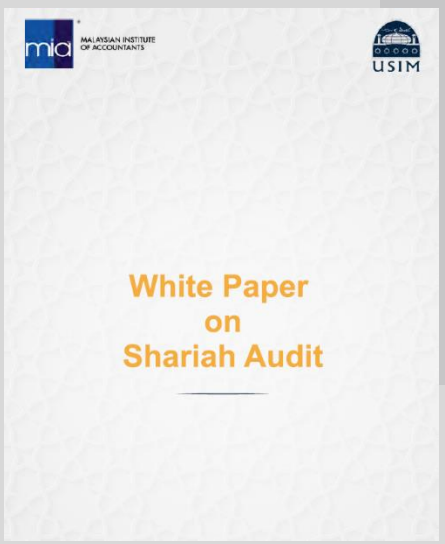
These challenges hinder the establishment of necessary functions for the practice of internal Shariah audit, leading to issues with the involvement of Internal Audit and Compliance Officers in Islamic Fund Management Companies, Real Estate Islamic Trusts, and Exchange Traded Funds, as well as Shariah Advisers' participation in review/audit processes.

Co-operatives.

Islamic co-operatives face challenges due to the absence of a specific Act governing their operations, which may result in non-compliance with Shariah principles or hinder the process of Shariah compliance. The effectiveness of existing mechanisms in ensuring adherence to Shariah principles and maqasid is questioned, and inconsistent practices, such as using different contracts for micro-financing, raise concerns.

Currently, ANGKASA conducts audits for co-operatives seeking Shariah-compliant product status, but the adoption of Shariah governance guidelines (GP28) issued by Suruhanjaya Koperasi Malaysia is not mandatory.

Exploration of Shariah governance mechanisms at the KOPSYAANGKASA level serves as a benchmark for other co-operatives.



White Paper on Shariah Audit

Enhancing multi-dimensional governance in Islamic co-operatives is crucial for maintaining Shariah compliance and protecting the rights of all parties involved. The integration of Shariah compliance within broader corporate governance frameworks is essential for addressing these challenges effectively.

- Public Trust Entities (PTEs).

Takaful Malaysia and YaPEIM solely invest in Shariah-compliant companies and have Shariah advisory committees and units overseeing investments. However, there is no documented evidence of specific Shariah audits in their reports or websites. These entities should consider establishing dedicated Shariah audit teams to ensure strict adherence to Shariah-compliant investments.

EPF and PNB invest in both conventional and Shariah-compliant companies and need to cleanse dividends from non-compliant declared securities. They have internal Shariah governance frameworks to oversee this process, including the establishment of Shariah units and Advisory Councils. Despite having internal audit departments, EPF and PNB lack dedicated internal Shariah audit units. As fund managers, PTEs face issues similar to those discussed in the Islamic capital market sector.

- State Islamic Religious Councils (SIRCs).

Implementing Shariah audit in Shariah-compliant Institutional and Related Institutions (SIRCs) and entities like zakat and waqf institutions presents challenges.

The focus of SIRCs on managing waqf, zakat, and Islamic social initiatives necessitates Shariah audit to enhance accountability and transparency, building public confidence in these institutions.

Current practices and challenges in SIRCs and related entities include integrating Shariah audit within the scope of internal audit, reporting to Internal Audit & Governance under the oversight of the Audit & Risk Committee. However, a lack of human capital with the necessary knowledge, skills, and experience for Shariah audit leads to challenges in budget allocation and compact audit plans.

The top three issues in implementing Shariah internal audit are inadequate implementation of risk-based Shariah internal audit, difficulties in identifying the scope of Shariah internal audit, and a shortage of available Shariah internal audit training programs in the market. Overcoming these challenges is essential for effective Shariah audit implementation in SIRCs and related institutions.

What should Internal Auditors do?

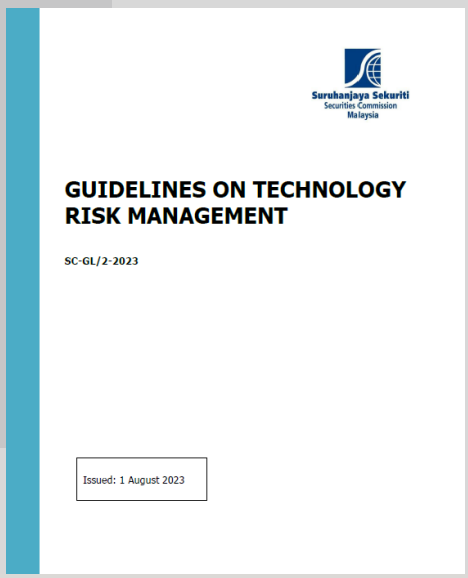
Standard 1200: Proficiency and Due Professional Care

Internal auditors are expected to possess the knowledge, skills, and competencies necessary to carry out their responsibilities. This includes having a good understanding of the organisation's industry, business processes, risks, and relevant laws and regulations. For Shariah audit in SIRCs and related institutions, proficiency would require auditors to have a strong grasp of Islamic finance principles, Shariah compliance requirements, and the specific operations and activities of these organisations.

References:

https://mia.org.my/knowledge-centre-resources/islamic-finance/

Guidelines on Technology Risk Management



Technology Risk Management Framework

Chapter 5: Governance.

- Board of Directors.

The board of a capital market entity must prioritise and provide oversight for managing technology risk as part of its overall risk management framework.

To fulfil this oversight role, the board is required to:

- Approve the Technology Risk Management (TRM) Framework and its policies.
- Define the risk appetite and risk tolerance statement for technology risk.
- Ensure the robustness and soundness of the TRM Framework and policies, commensurate with the entity's risk exposure.
- Oversee the implementation, review, and update of the TRM Framework and policies.
- Ensure strategies within the TRM Framework address the entity's technology risk exposure.
- Establish appropriate internal controls for TRM implementation.
- Assess the impact of technology risk before undertaking new activities, investments, or outsourcing arrangements.
- Allocate adequate resources for technology risk management and identify responsible persons in senior management.
- Ensure clear segregation of responsibilities and accountability for managing technology risk.
- Stay informed about new or emerging technology risk trends and understand their potential impact on the entity.

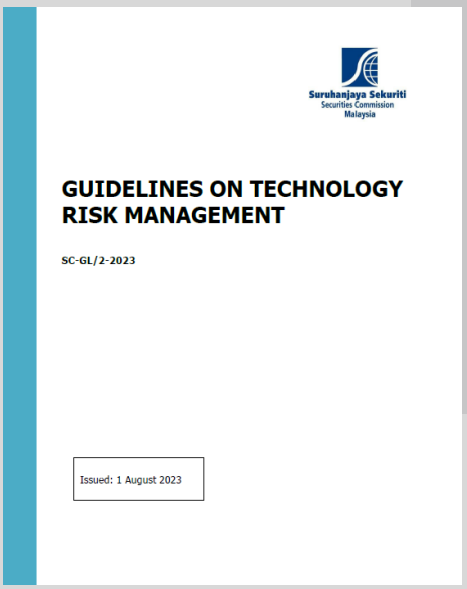
The board also holds accountability for the effectiveness of IT outsourcing arrangements and must ensure compliance with outsourcing policies and procedures.

- Senior Management.

The senior management of a capital market entity has various responsibilities concerning technology risk management, including:

- Developing and implementing a robust TRM Framework and policies commensurate with the entity's risk exposure for achieving security, reliability, and resilience of its IT operating environment.
- Approving and implementing robust technology risk management procedures that align with the entity's risk exposure and objectives.
- Regularly reviewing and updating technology risk management procedures, at least annually, for approval.
- Formulating and implementing segregated lines of responsibilities and accountability across all levels and functions, approved by the board.
- Ensuring employees, agents, and third-party service providers understand the TRM Framework, policies, and procedures, as well as their roles in managing cyber threats.
- Recommending appropriate strategies and measures to manage technology risk, including policy and procedure changes.
- Regularly reporting to the board on key technology risk, cyber breaches, business impact analysis, and critical technology operations.
- Providing the board with regular updates on cyber security issues, risk, and compliance with the cyber security framework.
- Reviewing, tracking, and reporting material deviations from the TRM Framework and policies to the board.
- Keeping the board informed about new and emerging technology risks relevant to the entity's risk appetite.
- Implementing approved remedial actions effectively and promptly.

Guidelines on Technology Risk Management



- Cybersecurity Awareness and Training.

A capital market entity must ensure that its board, senior management, employees, and agents, if any, attend cybersecurity awareness training at least annually. This training aims to enhance their awareness and preparedness to address various cyber risks effectively and fulfil their roles in safeguarding the entity's cybersecurity.

- Technology Audit.

A capital market entity must establish a technology audit plan to provide appropriate coverage of critical technology and conduct regular technology audits. The frequency of the audits should align with the business model, risk appetite, and level of technology dependency of the entity.

The technology audit must assess whether the entity's information systems comply with applicable laws, regulatory requirements, and industry guidelines. It should also evaluate the confidentiality, integrity, and availability of data and information, as well as the efficiency and effectiveness of IT service operations.

The auditors conducting the technology audit must possess the necessary competency, knowledge, and experience to perform the audit effectively.

The technology audit report should include an independent and objective opinion on the effectiveness of risk management, governance, and internal controls related to existing and emerging technology risks. The outcome of the technology audit must be reported to the board.

- Chapter 6: Technology Risk Management.

A capital market entity must establish and implement a robust and effective TRM Framework to manage its technology risk effectively. The TRM Framework and associated policies and procedures must be reviewed and updated periodically, with at least one review every three years.

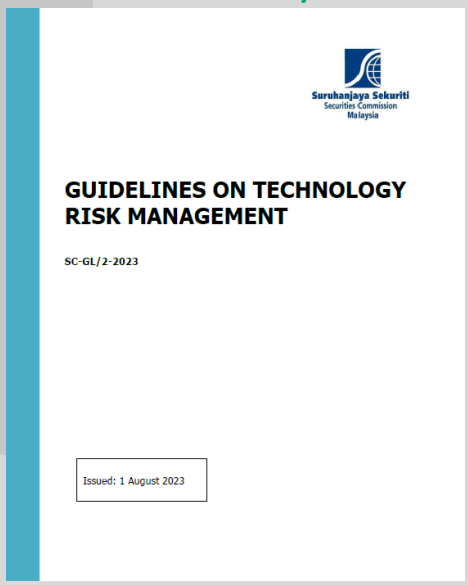
The entity must have an internal compliance process to ensure adherence to the TRM Framework, policies, and procedures, with deviations requiring approval from senior management based on appropriate justifications and alternative solutions or timelines.

The Technology Risk Management framework should include risk identification, assessment, mitigation, monitoring, review, and reporting for all existing and emerging technologies used by the entity.

Risks must be assigned to appropriate risk owners responsible for implementing proper risk treatment plans, and residual risks after treatment should be managed according to defined risk acceptance criteria.

The entity must maintain a board-approved key technology risk register for monitoring and reporting technology risk. Regular reviews of risk exposures and associated controls are essential for effective technology risk management.

Guidelines on Technology Risk Management



Chapter 7: Technology Operations Management.

- Technology Project Management.

A capital market entity must establish and implement clear and comprehensive internal guidelines for technology project management to ensure clarity, alignment, traceability, and effective resource utilisation during project completion.

The entity must conduct post-implementation reviews (PIR) on all critical technology and technology-related projects, using the PIR findings to enhance project management.

Risk assessments must be conducted to identify, manage, and monitor risks arising from critical technology projects throughout their life cycle, as project risks can impact project delivery timelines, budgets, and deliverable quality.

For technology-related projects, the entity must ensure adequate personnel, including key stakeholders, are involved in overseeing and managing the projects, with some individuals serving as project coordinators.

- System Acquisition and Development, System Testing and Acceptance and Access Control Management

A capital market entity must establish and implement internal processes encompassing system acquisition and development, system testing and acceptance and access control management.

- System Acquisition and Development.

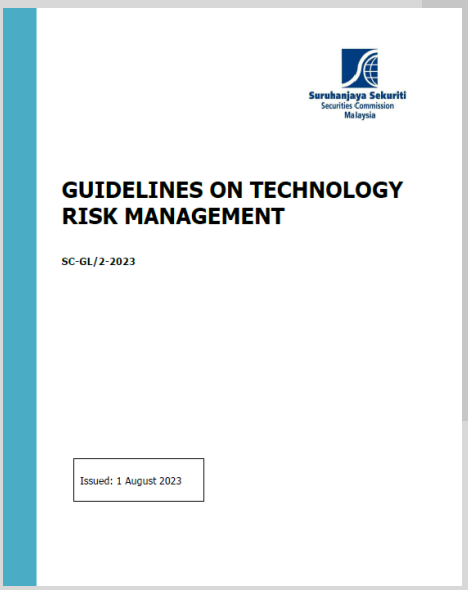
A capital market entity must establish and implement clear requirements and processes for managing its System Development Life Cycle (SDLC), covering planning, requirement analysis, design, implementation, testing, and acceptance. This includes requirements and processes for vendor selection and evaluation of systems, as well as assessing software development by vendors and in-house developers to ensure security and quality assurance.

Where possible, the entity should enter into a source code escrow agreement for critical systems to ensure accessibility. If not feasible, an appropriate alternative must be identified. Security requirements must be incorporated into system design to enable constant security evaluation and compliance with security practices throughout the SDLC to minimise vulnerabilities and reduce risk exposure. These security requirements should cover main control areas such as access control, authorization, data integrity and confidentiality, logging system activity, tracking security events, and handling exceptions.

- System Testing and Acceptance.

A capital market entity must establish a rigorous system testing methodology to ensure that systems meet user requirements and perform as intended before deployment. Testing must cover business logic, function, controls, and performance under various load and stress conditions. Automated testing methodology is encouraged where feasible to ensure comprehensive testing scopes as part of the testing strategy. All issues identified during testing, including vulnerabilities, deficiencies, system defects, or software bugs, must be properly documented, tracked, and addressed.

Guidelines on Technology Risk Management



Issues that could adversely impact the entity's operations or service delivery to clients must be reported to senior management and rectified before system deployment to the production environment.

The entity must perform final acceptance testing focusing on technical aspects and user acceptance testing focusing on functional aspects to ensure the system is production-ready and meets documented requirements.

Results of the final acceptance and user acceptance testing must be reported to senior management. For acquired systems, the entity must ensure the final approved version is used for implementation after addressing changes during testing by the vendor.

- Access Control Management.

To minimise the risk of unauthorised access to information assets, a capital market entity must:

- Establish user access management policies and procedures to provide, modify, and revoke access rights to IT systems based on users' roles and responsibilities. The access matrix should be periodically reviewed.

- Enforce and periodically review password controls to enhance system resilience against attacks.

- Enable logging facilities to capture user logins, system activities, privilege accounts, and service accounts for audit and investigation purposes. Regular log reviews should be conducted to identify irregularities.

The entity must also use strong fraud deterrents, such as multi-factor authentication (MFA) and privilege access management, for sensitive system functions to safeguard systems and data from unauthorised access on a best-effort basis.

What Internal Auditors should do?

Standard 2120 - Control Environment

The internal audit function plays a crucial role in evaluating and assessing the adequacy and effectiveness of control policies and procedures.

This includes user access management policies and procedures, which ensure that access rights and privileges are granted based on the roles and responsibilities of users. Internal auditors can review and assess the design and implementation of these policies and procedures to ensure they align with best practices and regulatory requirements.

In addition, the *Standard 2120 – Control Environment* also guides internal auditors in assessing the effectiveness of the control environment and risk management practices related to information security and access controls. By evaluating these practices, internal auditors can help organisations strengthen their control environment, minimise the risk of unauthorised access to information assets, and enhance overall cybersecurity measures.

References:

https://www.sc.com.my/api/documentms/download.ashx?id=1d694317-0cc0-4e67-bbd7-c9549441c5a1

Audit Advantage: How IA assists management in unlocking growth

***NEW SECTION* - TECHNICAL WRITER**

BY JAVEN KHOO AI WEE, CIA, CISA, CFE, CC
CMIIA Membership No. 211787

CONTEXT

Sales and Marketing (S&M) function has always been a favourite audit area as it has direct impact to an organisation's bottom-line hence, business prosperity and sustainability. More so for a business sector that is highly competitive such as property development during the challenging COVID-19 pandemic. Market jittery has resulted in cautious spending especially on big ticket items like property purchase.

Accordingly, an audit has been conducted during January-February 2021 with the objective to assess: -
- adequacy of governance design in supporting business objectives.
- effectiveness of Sales & Marketing strategy implementation in maximising value; and
- effectiveness and efficiency of processes in improving pace and agility to market.

ASSURANCE CONDUCT

Kindly note that some details have been generalised, aggregated, or modified due to data sensitivity.

IA provides valuable insights into an organization's processes, highlighting areas for improvement and efficiency gains. By examining existing processes, controls, and workflows, IA helps identify bottlenecks, inefficiencies, and opportunities for optimization.

(a) Adequacy of governance design in supporting business objectives

In assessing Client's **market strategy development process for robustness**, IA evaluated if the said process and decision-making are risk assessed, supported by solid business case, and approved by the correct level of authority. Since S&M is very much customer-facing, exacerbated by the need to "Know Your Customer" as part of compliance with Third Party Risk Management (TPRM), **careful management of customer's confidential information** is imperative. Hence, IA also evaluated the Client's system of internal controls in **preventing leakage of customer's personal data**, such as:-

- compliance with Personal Data Protection Act (PDPA), and General Data Protection Regulation (GDPR), where applicable.
- logical access controls to its customer data repository system.

Equally important is the timeliness and reliability of management reporting, especially in **identifying critical business issues for prompt escalation** to management for effective steering or intervention. Business objectives were also reviewed for **effective cascading into S&M's balanced scorecard**. This could be of particular interest especially during pandemic because unrealistic KPIs or targets may lead to work pressures that fit into the fraud triangle, **potentially increasing the risk of fraud within an organization**.

- *Pressure*: unrealistic KPIs can create **a sense of desperation and financial strain** hence, become a motivating factor for employees to resort to fraudulent activities as a means to meet targets and avoid negative consequences.

- *Opportunity*: unrealistic KPIs may incentivise employees to **find shortcuts or engage in unethical practices to attain the desired results**, eg. tempted to manipulate data, fabricate records or engage in other fraudulent activities to meet their targets while evading detection.

- *Rationalisation*: unrealistic KPIs can provide employees with a justification for fraudulent behaviour, arguing that they were **merely doing what was necessary to meet management expectations or protect their jobs.**

Unrealistic KPIs alone do not cause fraud, but the combination of the above three (3) elements can lead to the potential for fraud. Hence, organisations should **establish realistic and attainable KPIs** and ensure that employees are not subjected to excessive pressures, including **promoting a culture of open communication and transparency**, and **implementing robust internal controls and monitoring mechanisms** to deter and detect fraudulent activities.

(b) Effectiveness of Sales & Marketing strategy implementation in maximising value

The pandemic has generally transformed the way of working for most organisations if not all, where **creativity and agility were tested**. Hence Client has also jumped on the **digital bandwagon in reaching and engaging with its potential buyers**, eg. *metaverse* (virtual property tours, 3D modelling, live video streaming, etc.), digital marketing platforms, targeted online advertising, e-booking system, online chat support, etc. – to name just a few.

- On this note, IA has performed **benchmarking** on a few sampled close competitors by **visiting their digital domains** and **acted as "mystery buyers"** to solicit information on their product value propositions, sales incentives, sales progress, etc for **comparative analysis** purpose.

Client's **data analytics** in performing customer profiling, market segmentation and positioning were also assessed for effectiveness in supporting the marketing strategy.

- From the assessment, IA has **identified a key market with income stability and high purchasing power that has been under-tapped** as evidenced by the segment's declining trend of property purchase during 2016-2020.

  In order to serve as a **Strategic Business Partner**, IA has conducted a **survey** on this segment to solicit feedbacks on their awareness of Client's branding and promotional activities (ie. top-of-mind awareness), property preferences, satisfaction from any prior purchase, etc. In addition, IA went the **extra mile** in asking respondents if they would like to be contacted to know more about Client's property launches (PDPA requirements duly observed).

  - At end of the survey, IA has **handed to Client approximately 400 sales leads from the under-tapped yet prospective segment**, not to mention the **insights gathered from the survey results on rooms for future improvement on communication channels, product specifics, promotional offers, etc.**

(c) Effectiveness and efficiency of processes in improving pace and agility to market

Some of the key procedures governing Client's S&M activities are with regards to sales launch implementation, development of Sales & Purchase Agreement (SPA), Advertising Permit and Developers License (APDL) application, customer complaint and defect management (CRM), etc. These were assessed for improvement opportunities to **shorten end-to-end development cycle and improve speed to market.** Afterall, S&M provides key inputs from market to its counterparts in property development and planning.

As **social media** was leveraged heavily by Client for its marketing campaigns, IA also evaluated the comments and queries raised by both prospective and existing customers, and ultimately:-

- how effective and efficient was the Client in **boosting customer's confidence, satisfaction and loyalty.**

  The review also included whether any negative comment or customer complaint received has been hidden or removed by the focal person because this may aggravate the complainants and accelerate the spread of negative word-of-mouth which may ultimately hamper S&M efforts for future projects.

- whether **quality or design complaints** have been **forwarded to the relevant parties** for immediate action and future improvement.

In addition, the **CRM system** was evaluated for **reliability and effectiveness**, eg. system upgrade including patch management, segregation of duty controls, access controls, system logs, etc. Likewise on the **utilisation of CRM system for monitoring and management reporting**, IA assessed the dashboards and data analytics performed on aging of queries and complaints closure, defect rectification turnaround time, etc for **performance management** and **lessons learnt for continuous improvement.**

KEY TAKEAWAYS

- The above testimony shows how IA can provide valuable insights and support business objectives beyond traditional auditing responsibilities. IA's proactive approach such as benchmarking competitors, customer surveying and generating sales leads are just some of the ways to value-add as a Strategic Business Partner.

- The pandemic has accelerated the adoption of digital S&M platforms and tools as the "current normal", hence should be further leveraged for future success. Equally important is for data analytics to support decision making. *"In the world of big data, it is essential to move from merely collecting information to discovering actionable insights" – Bernard Marr".*

- The fraud triangle is one of the many models that explains the contributing factors to occurrence of fraud within an organisation. Although all three (3) elements of *Pressure, Opportunity* and *Rationalisation* need to be present for fraud to take place, it is important to note that the presence of all these elements is not a guarantee that fraud will occur. Rather, it increases the likelihood of fraudulent behaviour. Amongst others, adequate and effective internal controls could deter fraudulent behaviour by reducing the Opportunity for fraud to take place.

(word count: 1,250)