KPMG

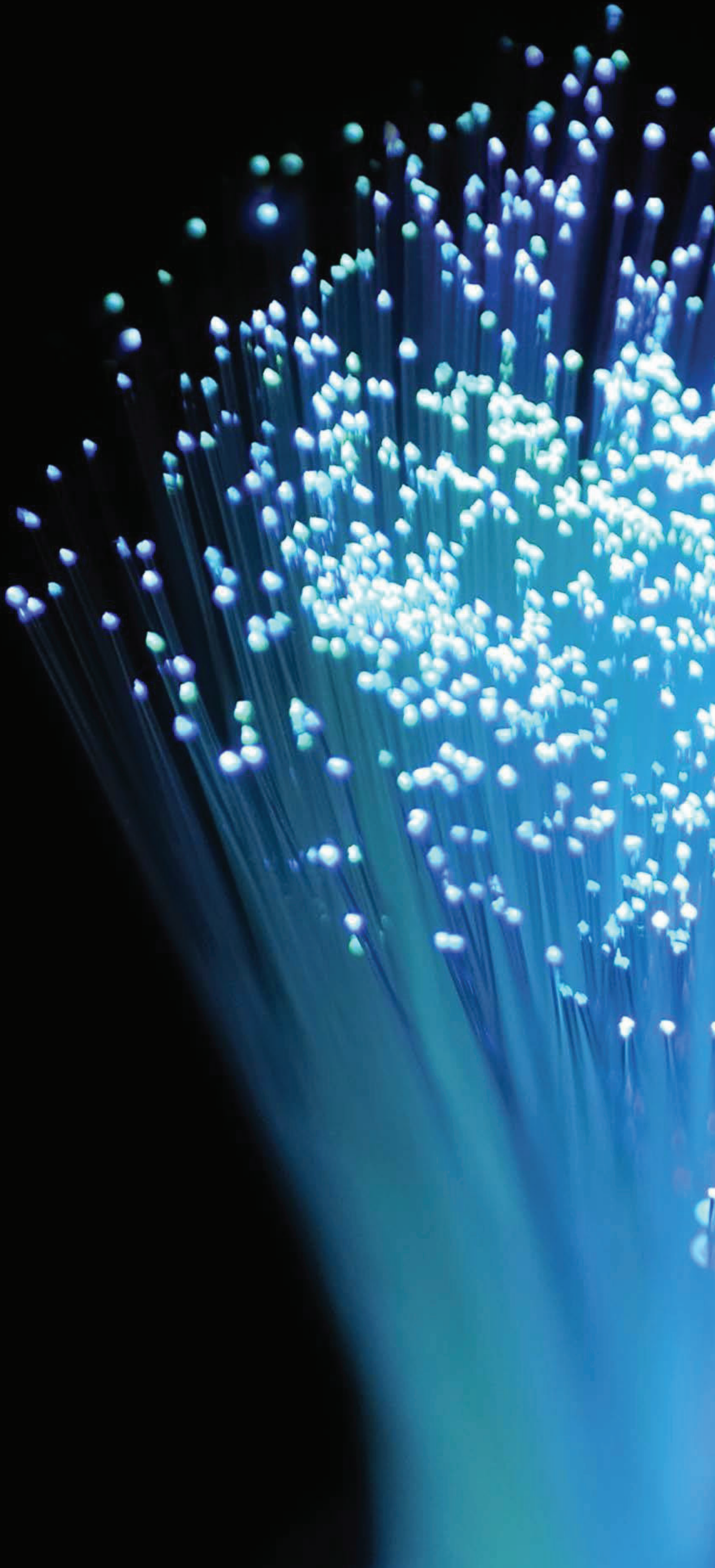
MIoD Mauritius Institute of Directors

Promoting Corporate Governance across the board

Audit Committee Forum

Position Paper 5

Guidelines for the Audit Committee's approach to Information Technology risk



July 2017

About the Audit Committee Forum

Recognising the importance of Audit Committees as part of good Corporate Governance, the Mauritius Institute of Directors (MIoD) and KPMG have set up the Audit Committee Forum (the Forum) in order to help Audit Committees in Mauritius, in both the public and the private sectors, improve their effectiveness.

The purpose of the Forum is to serve Audit Committee members and help them adapt to their changing role. Historically, Audit Committees have largely been left on their own to keep pace with rapidly changing information related to governance, risk management, audit issues, accounting, financial reporting, current issues, future changes and international developments.

The Forum provides guidance for Audit Committees based on the latest legislative and regulatory requirements. It also highlights best practice guidance to enable Audit Committee members to carry out their responsibilities effectively. To this end, it provides a valuable source of information to Audit Committee members and acts as a resource to which they can turn for information or to share knowledge.

The Forum's primary objective is thus to communicate with Audit Committee members and enhance their awareness and ability to implement effective Audit Committee processes.

Position Paper series

The Position Papers, produced periodically by the Forum, aim to provide Board directors and specifically Audit Committee members with basic best practice guidance notes to assist in the running of an effective Audit Committee.
This **Position Paper 5** deals with the Guidelines for the Audit Committee's approach to Information Technology (IT) risk.

Previous Position Papers issued:

- **Position Paper 1** (July 2014) sets out the essential requirements that should be complied with by every Audit Committee in accordance with the National Code of Corporate Governance.

- **Position Paper 2** (May 2015) sets out how the Audit Committee can accomplish its duties through a collaborative relationship with two of the Assurance Providers, notably Internal and External Auditors.

- **Position Paper 3** (December 2015) deals with the Audit Committee's role in control and risk management.

- **Position Paper 4** (October 2016) deals with the Guidelines for the Audit Committee's assessment and response to the risk of fraud.

Members of the Forum

Collectively, the Forum is made up of the following members drawn from diverse professional backgrounds with significant experience in both the private and the public sectors.

Gujadhur Anil – Chairman

Chan Moo Lun Kim Chow

Chung John

De Chasteauneuf Jerome

De Marassé Enouf Maurice

Dinan Pierre

Felix Jean-Michel

Fernandez Zara Juan Carlos

Goburdhun Khoymil

Ibrahim Nesmah

Koenig Fabrice

Leung Shing Georges

Molaye Sanjay

Ng Cheong Hin Christine

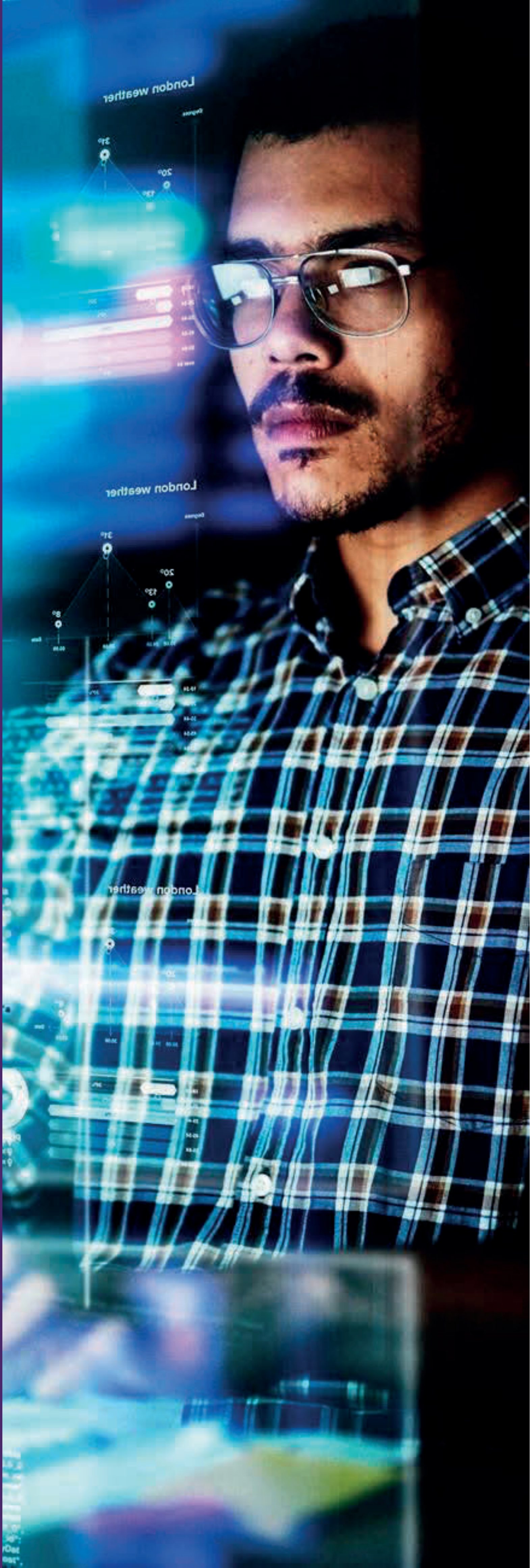
Ramdin-Clark Madhavi

Rojoa Nashreen

Ujoodha Sheila

Secretary:
Bishundat Varsha

Contents



Introduction

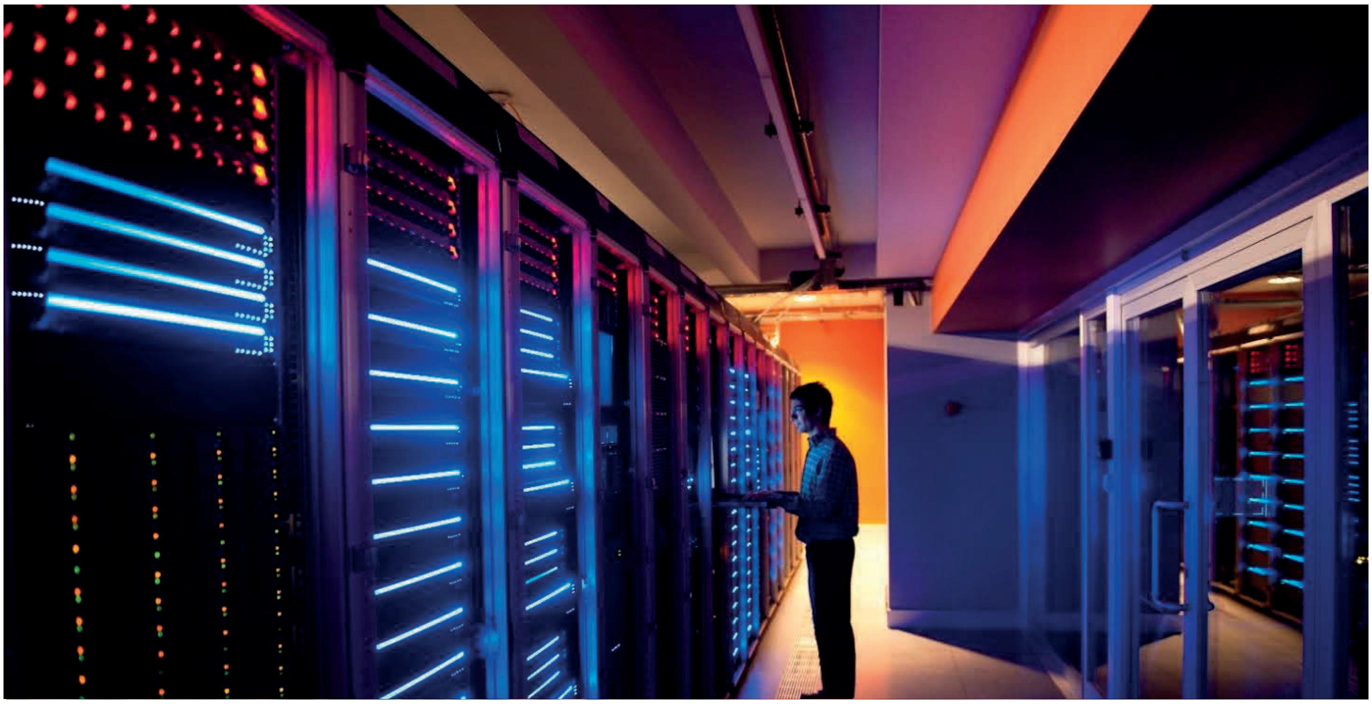
Information Technology (IT) governance is the shared responsibility of both the Board of Directors and Executive Management. It is an integral part of corporate governance and consists of the leadership and organisational structures and processes which ensure that the organisation's IT system efficiently and flawlessly sustains and extends the organisation's strategies and objectives. IT governance can be defined as a "framework that supports the effective and efficient management of information resources to facilitate the achievement of corporate objectives. The focus is on the measurement and management of IT performance to ensure that the risks and costs associated with IT are appropriately controlled"[1]

For the purposes of this Position Paper, IT has been defined as the employment of an interconnected electronic technology, particularly computer and telecommunications systems or similar processes to flow, transmit, handle, store and retrieve information pertaining to execution of the regular business and interactions of the enterprise.

The Audit Committee Forum is aware that corporate governance structures are not the same in every organisation. Governance principles should be applied and structured to best suit the size and complexity of the organisation, including IT governance. Nevertheless, irrespective of the organisation's size and importance, board and management are expected to put in place a fully performing and cost-efficient IT platform free from systemic risk.

This position paper is written on the basis that the Audit Committee is responsible for the oversight of risk management in the organisation and that this duty does not devolve on a separate Risk Committee.

The Audit Committee is always responsible for oversight of internal controls, including general and application IT controls. This oversight function involves ensuring the organisation has an appropriate framework of controls which are appropriately documented and that systems are in place to ensure the controls operate effectively. It includes ensuring that the organisation always has a specified IT- risk owner who will periodically report to the Board on the ongoing status of the IT system, according to a clearly and comprehensively documented job specification.



[1]. Source: Ken Doughty and Frank Grieco, "IT Governance: Pass or Fail?" Information Systems Control Journal 2, 2005

The role of the Audit Committee

IT plays an ever-increasingly important role in supporting business processes as well as enabling entities to differentiate themselves in the marketplace. With time, increasing reliance is also being placed on systems and other automated control processes to manage risk. Questions have been raised regarding the role of the Audit Committee in monitoring the associated increased IT risks.

The Board of Directors is responsible for the strategic direction and decisions regarding IT and the Audit Committee is responsible for the oversight of some strategic and operational aspects of IT, particularly IT risks. Principle 4 of the Code of Corporate Governance for Mauritius 2016, specifically states that 'The Board is responsible for the governance of the organisation's information strategy, information technology and information security'.

The Audit Committee should, in the case of all entities, determine whether IT plays a critical role to safeguard the enterprise against existing and foreseeable risks relating to the internal security of the system and its effectiveness to deliver in a timely manner, expected outcomes in relation to third parties dealing with the enterprise. The aspects in which the Audit Committee plays an oversight role include:

(i) IT risks and controls

The Audit Committee should consider IT risks as a crucial element pertaining to the effective oversight of risk management of the organisation. They should ascertain whether they are adequately equipped with the specialist technical know-how necessary to review and analyse the effectiveness of systems and systems controls. Even if that is the case, the Audit Committee may still need to rely on expert advice from within or outside the organisation to be able to deal with issues as and when they arise and even before they arise. Management / IT technicians' advice should be delivered to the Audit Committee / Board of Directors in plain language, avoiding industry and technical jargon so that explanations are fully understood as to implications and key issues.

In understanding and measuring IT risks, the Audit Committee should take a comprehensive view of the organisation's overall exposure to IT risks from a business perspective, including the areas of the business which are most dependent on IT for their effective and continual operation. But that does not mean that security threats to the organisation's IT system cannot emanate from other less important areas, including the amount of free access insiders have to the system.

Areas that are highly dependent on IT are more exposed if IT risks are not appropriately governed. In such a case, the Audit Committee would need to obtain appropriate independent assurance that controls are adequate to address these risks.

The most widely adopted framework in the oversight of IT risks and controls is COBIT (Control Objectives for Information Technology). COBIT 5 provides a comprehensive framework that assists enterprises to achieve their goals and deliver value through effective governance and management of an enterprise's IT system. The COBIT 5 principles and enablers are generic and useful for enterprises of all sizes, in commercial, not-for-profit or public sectors. An overview of COBIT framework is provided in Appendix A.

Another possible framework is the ISO 27002, published by the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC). Appendix B provides an overview of the ISO 27002 and its key controls.

Some of the main IT risks facing entities are listed below:

— IT outsourcing: increasingly, entities are outsourcing their IT structures and systems. Reliance on outsourced facilities raises additional concerns for effective IT risk management

— Enterprise Resource Planning systems: these systems are increasingly becoming more complex and costly to implement. The key risks include:

  - Overall project failure;
  - Project running over budget and time;
  - Failure to deliver the expected return on investment; and
  - Insufficient administrative and management skills due to budget / other constraints.

> “The Board is responsible for the governance of the organisation's information strategy, information technology and information security”

— System changes and implementation: Often, the process of software changes and implementation of new systems results in increased IT-related risks. These include the selection of the appropriate software, the appropriate implementation process and the integrity of information. The Audit Committee, although not responsible for the decision for system changes and implementation, should ensure that the process for establishing the needs assessment is rigorous and that adequate planning is undertaken for the change or conversion. It should consider the risk of rapid obsolescence of systems acquired and whether they are being appropriately overhauled / replaced due to risks posed and / or changes in technology

— Tailor-made software increases the risk to the organisation significantly, as the organisation ordinarily does not have access to the source codes, i.e. subsequent changes cannot be made and / or the initial developer no longer exists. A practical solution to this issue is to place the codes in escrow to ensure that access to the source codes will be maintained. It is also vital that Internal Audit be involved before and after implementing a new system or changing an existing system

— Access is one of the most problematic areas in a modern business environment, driven by and highly dependent on IT. Some of the areas of concern include:

- Lack of discipline in changing and protecting passwords;

- Inappropriate access levels assigned to staff which allows for abuse of information;

- Lack of discipline in removing access of previous employees;

- Risk associated with remote access to information through Wi-Fi and Broadband networks;

- Inappropriate access and authority of super-users. Enterprises should exercise control by maintaining and reviewing an updated register of all super-users with the various access levels assigned to them;

- Unauthorised users try to break into systems by a phishing attack.

— Cyber security, denial of service attack, malware and logical attacks

— Cloud Computing - Cloud services purchased without consultation and involvement of IT personnel

— Access by mobile devices (Connecting your personal device into the system carries the high risk of losing sensitive data and information).

(ii) Business continuity related to IT

The reliance on IT has raised the need for better disaster recovery planning. It is important that the Audit Committee questions Management with regard to the business continuity plan as part of the oversight role.

(iii) Information security and privacy

Rapid technological advances have led to instantaneous availability of information, often across several geographical locations. The use of removable storage devices and mobile e-mail solutions have increased the risk of unauthorised access to sensitive and confidential enterprise information, including through hacking.

Appendix C provides detailed questions which the Audit Committee can ask to evaluate whether the IT risks are properly addressed.

Action plan for the Audit Committee

Management is responsible for identifying risks and subsequently developing, assessing and monitoring appropriate internal controls. The Chief Executive Officer (CEO), Chief Financial Officer (CFO), and Chief Information Officer (CIO), should provide the relevant assurance regarding IT risks and controls in place to the Audit Committee in plain language. The Audit Committee should ensure that Management is performing ongoing assessments of all IT risks and be satisfied that these risks are adequately addressed.

The Audit Committee's oversight of IT risks can be facilitated through the following steps:

- **Updating the Audit Committee Charter**
  Audit Committees and Boards need to align their oversight responsibilities for IT governance and agree on a workable arrangement that makes the most sense for the culture and governance structure of the company. This should clearly be addressed in the charters of the Board and the Audit Committee.

- **Utilise direct access to the CIO**
  Through presentations by the business unit heads and the CIO, or equivalent IT executive, it is possible for the Audit Committee to understand, from a business perspective, how extensively IT is being utilised in all areas of the business, and what is the potential exposure from IT risks.

  The Audit Committee should receive a comprehensive plan from the CIO, or equivalent, comprising an assessment of the IT function and any key weaknesses in IT controls. The CIO, Internal Audit and External Audit, should provide the Audit Committee with assurance that IT is being properly managed and that IT risks are being controlled. The Audit Committee may request the CIO to sign a representation letter to that effect.

— **Utilise internal audit support**
Internal Audit normally has a degree of IT knowledge and sophistication consistent with the types of IT risks faced by the organisation. It should be utilised to extensively test controls. Where Internal Audit does not have the necessary appropriate IT skills and knowledge, the Audit Committee should consider outsourcing this assessment to qualified and reliable third parties.

The Audit Committee should ask Internal Audit to answer the following questions:

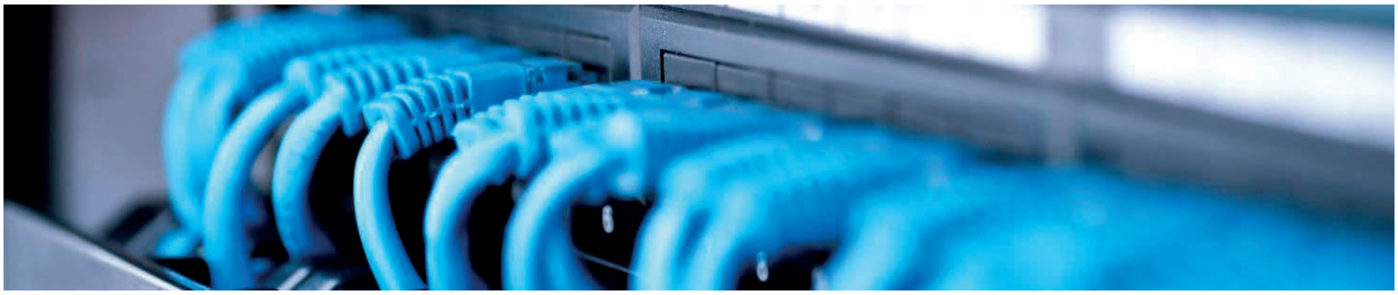
- Has Internal Audit come across any recent breach of the IT system? Were actions taken to prevent recurrence?
- What is the level of reliance on IT personnel, considering both key reliance and level of skill? [People risk]
- How is the organisation's management securing data? [Information risk]
- How reliable are the IT systems (both applications and infrastructure)? [Integrity of information and Availability risk]
- What is the level of dependency on IT managed by third parties and how is the organisation managing associated risks? [Outsourcing risk]
- What regulation / legislation applies to IT and how well has the IT function been designed to help the organisation comply with relevant regulations and legislations? [Legal risk]
- Is Internal Audit aware of all changes made to the IT system and are these conversions monitored? How much change is being effected (and managed) on the IT structure of the organisation? [Change and project management risk]
- Is the internal control environment sufficiently robust to allow Internal Audit to supply the Audit Committee with a representation?

— **Utilise External Audit support**
In the modern complex business environment, External Audit cannot be performed without an assessment of IT controls (both general and application). The Audit Committee should receive comfort from External Audit that the IT risks and controls were assessed as part of their process. The Audit Committee should obtain an understanding of the extent of the IT-related testing and evaluation performed by them and should, inter alia, ask:

- How much reliance is External Audit placing on the IT system?
- How often has External Audit defaulted to substantive testing to gather audit evidence?

— **Adopt a documented framework for assessing IT risks**
The COBIT framework is one of the possible frameworks that allows for effective and efficient risk management with objective quantifiable assessment of all significant IT risks (Appendix A).

— **Communication**
Once Management has assessed and mitigated the key IT risks by designing and implementing appropriate controls, the Audit Committee (with the help of Internal Audit or other independent service providers) should critically review the IT risk assessment and the designated controls. The controls should be sufficiently comprehensive and appropriate to provide the necessary assurance and this broader perspective may be useful in identifying gaps in them. The Audit Committee should also receive feedback from both Internal and External Audit with regard to IT risks and weaknesses in internal controls.



Conclusion

The use of IT in businesses has become pervasive. This trend will most likely continue in the future. Accordingly, businesses will be ever more exposed to risks associated with extensive use of IT, including online and offline risks. No doubt, enterprises will take maximum security measures to avoid business disruption due to unauthorised or malevolent intrusion in the IT system. As this is a dynamically evolving platform, risks will be expected to assume different forms over time, capable of putting a business at serious operational, legal and monetary risks.

The situation calls for sustained vigilance on the adequacy and reliability of the IT system, at the risk of serious business disruption, material loss and loss of credibility vis-à-vis the public and counterparties. The Audit Committee may or may not be equipped to monitor the technology risks involved. However, it can resort to assigning explicit responsibilities to specified officers within the organisation to maintain the system in good health and to report regularly any incidents which threaten business integrity from the IT angle for timely preventive action to be taken.

Irrespective of whether it is entrusted by the Board to also undertake risk management, the Audit Committee must ensure as part of its ordinary duties that IT risks are fully contained, optimal use is being made of available systems and processes and that exaggerated expenditures are being avoided. IT systems are becoming increasingly porous despite precautions taken to ward off intruders. This makes it even more challenging for the Audit Committee to spot failings and take actions before any harm is actually done to the detriment of the enterprise. A proactive approach will help the enterprise improve its efficiencies and ensure safe delivery of outcomes in this new technology age.

Appendices

Appendix A

Overview of COBIT Framework

COBIT 5 has been built around five major principles for Governance and Management of the IT of an enterprise. They should enable it to build an effective governance and management framework that optimizes information and technology investment and use for the benefit of its stakeholders.

COBIT 5 Principles

Based on five principles and seven enablers, COBIT 5 uses governance and management practices to describe actions that are examples of good practices to effect governance and management over the enterprise IT. Many of these practices and the supporting activities exert 'control' over the process to deliver the required outcome.

COBIT 5 Principle 1: Meeting Stakeholder Needs
It is critical to define and link Enterprise goals and IT-related goals to best support stakeholder needs.

COBIT 5 Principle 2: Covering the Enterprise End to End
An enterprise must shift from managing IT as a cost to managing IT as an asset, and its managers must take on the accountability for governing and managing IT-related assets within their own functions.

COBIT 5 Principle 3: Applying a Single Integrated Framework
Using a single, integrated governance framework can help an enterprise deliver optimum value from its IT assets and resources.

COBIT 5 Principle 4: Enabling a Holistic Approach
Governance of Enterprise IT (GEIT) requires a holistic approach that takes into account many components, also known as enablers who influence whether something will work. COBIT 5 features seven enablers for improving GEIT, including principles, policies and frameworks, processes, culture, information and people.

COBIT 5 Principle 5: Separating Governance from Management
Governance processes ensure goals are achieved by evaluating stakeholder needs, setting direction through prioritisation and decision making; and monitoring performance, compliance and progress. Based on the results from governance activities, business and IT management, an enterprise should then plan, build, run and monitor activities to ensure alignment with the direction that was set.

COBIT 4.1 Control Objectives

To govern IT effectively, it is important to appreciate the activities and risks within IT that need to be managed. The COBIT 5 governance or management practices are equivalent to the COBIT 4.1 control objectives detailed below; they are usually ordered into the responsibility domains of plan, build, run and monitor.

(i) Plan and Organise

This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. The realisation of the strategic vision needs to be planned, communicated and managed for different perspectives. A proper organisation as well as technological infrastructure should be put in place. This domain typically addresses the following management questions:

- Are IT and the business strategy aligned?
- Is the enterprise achieving optimum use of its resources?
- Does everyone in the organisation understand the IT objectives?
- Are IT risks understood and being managed?
- Is the quality of IT systems appropriate for business needs?

(ii) Acquire and Implement

To realise the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure that the solutions continue to meet business objectives. This domain typically addresses the following management questions:

— Are new projects likely to deliver solutions that meet business needs?
— Are new projects likely to be delivered on time and within budget?
— Will the new systems work properly when implemented?
— Will changes be made without upsetting current business operations?

(iii) Deliver and Support

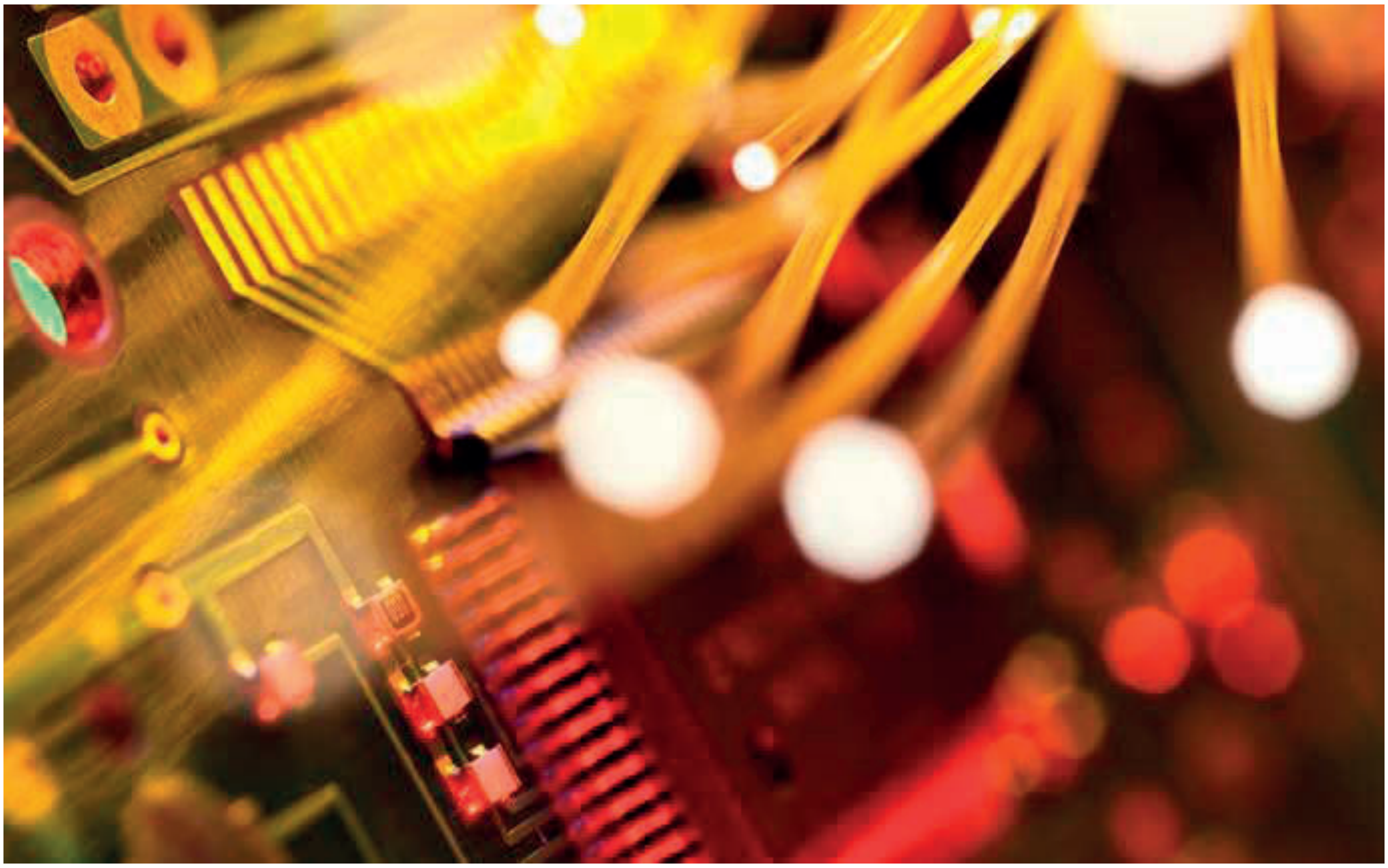
This domain is concerned with the delivery of required services, which includes service delivery, management of security and continuity, service support for users, and management of data and operational facilities. It typically addresses the following questions:

— Are IT services being delivered in line with business priorities?
— Are IT costs optimised?
— Is the workforce able to use the IT systems productively and safely?
— Are adequate confidentiality, integrity and availability in place for information security?

(iv) Monitor and Evaluate

All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain addresses performance management, monitoring of internal control, regulatory compliance and governance. It typically addresses the following management questions:

— Is IT performance measured to detect problems before it is too late?
— Does Management ensure that internal controls are effective and efficient?
— Can IT performance be linked back to business goals?
— Are adequate confidentiality, integrity and availability controls in place for information security?



Appendix B

Overview of ISO 27002 framework

	Section of ISO 27002	Controls as per ISO 27002
1	**Information Security Policies**	Policies on information security should be defined, approved by Management and communicated to employees. Policies on information security should be reviewed at planned interval or when significant changes occur.
2	**Organisation of Information Security**	Information security responsibilities should be defined and allocated. Areas of responsibility should be segregated.
3	**Human Resource Security**	Responsibilities for information security should be mentioned in the contracts of employees. Awareness education / training and updates in policies should be provided to all employees.
4	**Asset Management**	Assets associated with information and information processing facilities should be identified and inventoried. Ownership and responsibilities of assets should be clearly defined and communicated. Information should be classified in terms of sensitivity and legal requirements and a set of procedures for information labelling should be established.
5	**Access Control**	An access control policy is established and reviewed based on information security requirements. A policy is formulated concerning the use of networks and network services. User access rights are reviewed at regular intervals. Access rights are removed upon termination of employment or adjusted upon change. A formal user registration and de-registration process is implemented to enable assignment of access rights. Password management systems should be interactive and ensure quality passwords. Access to systems and applications should be controlled by a secure log-on procedure.

	Section of ISO 27002	Controls as per ISO 27002
6	**Cryptography**	A policy on the use of cryptographic controls for protection of information should be developed and implemented. A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle.
7	**Physical and Environmental Securities**	Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. Physical security for offices, rooms and facilities should be designed and applied.
8	**Operations Security**	Detection, prevention and recovery controls to protect against malware should be implemented. Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy. Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed. System administrator and system operator activities should be logged and the logs protected and regularly reviewed. Technical vulnerabilities should be evaluated, addressed and reported timely.
9	**Communications Security**	Security mechanisms, service levels and management requirements of all network services should be identified and included in the IT Manual or outsourced services agreements. Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities. Requirements for confidentiality or non-disclosure agreements reflecting the organisation’s needs for the protection of information should be identified, regularly reviewed and documented.
10	**System Acquisition, Development & Maintenance**	The information security related requirements should be included in the new information systems or enhancements to existing information systems. A secure development policy should be defined and established. Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures.

	Section of ISO 27002	Controls as per ISO 27002
10	**System Acquisition, Development & Maintenance (Continued)**	A software update management process should be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorized software.
11	**Supplier Relationships**	A policy and information security controls should be established on supplier access to the enterprise information. Supplier agreements should be established and documented determining the information security requirements.
12	**Information Security Incident Management**	Procedures should be established to ensure a quick, effective and orderly response to information security incidents. Information security events should be reported through appropriate management channels. Information security events should be assessed and it should be decided if they are to be classified as information security incidents. Information security incidents should be responded to in accordance with the documented procedures.
13	**Information Security Aspects of Business Continuity Management**	Information security requirements and the continuity of information security management should be determined and documented in adverse situations. The Business Continuity framework should be maintained to ensure consistency. Information security continuity controls should be verified at regular intervals.
14	**Compliance**	All relevant legislations and regulatory / contractual requirements should be identified, documented and kept up-to-date. Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation. The organisation's approach to managing information security and its implementation should be reviewed independently at regular intervals. Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies. Information systems should be regularly reviewed for technical compliance with the organisation's information security policies and standards.

Appendix C

Questions to evaluate IT risks

The Audit Committee may request the Internal Audit or CIO to use this questionnaire to ensure that IT risks are appropriately addressed. Feedback on these questions, and the questions listed in the position paper, should be provided to the Audit Committee to assist in its oversight responsibility.

1. Computer controls (Group IT)

a. Is the disaster recovery plan (DRP) for each site updated for all significant changes?
b. Is the DRP tested at least annually?
c. Does IT ensure that the backups at all sites are in fact up to date and tested?
d. Does IT check that the UPS's (uninterrupted power supply) are subject to regular services and logged?
e. Is virus-checking software loaded on all users that link to the internet?
f. Is the virus checking software loaded, maintained centrally and updated automatically daily?

2. Logical access

a. Are the password standards enforced using the operating system?
b. Is single sign-on used where possible?
c. Does each application enforce regular changes of passwords where they are unique to the application?
d. Does each application support the password standards?
e. Does the system enforce password changes when first logging on?
f. When users leave or are transferred, are the user profiles updated?
g. Is there an audit trail of all updates to user profiles?
h. Are files backed up and archived?

3. IT outsourcing

a. Does the organisation have an appropriate Service Level Agreement (SLA) with the service organisation?
b. Has the SLA been interrogated sufficiently and reviewed by relevant specialists, including legal, to ensure that the third party providers have bound themselves to adopt the level of data security this organisation requires?
c. Is the SLA sufficiently comprehensive for the nature and scale of business being undertaken by the organisation and is it being complied with? (Often Audit Committees request a compliance audit of the SLA for this purpose).
d. Has the organisation requested a report from the service organisation's auditors, confirming the effective operation of IT controls at the service organisation (an 'ISAE 3402-type' report)? In other words, do we have assurance that the service organisation is fully equipped and has been independently vetted to have the necessary track record of dealing with problems which may arise, in real time?

4. Business continuity related to IT

a. How critical is the IT system to the business? Is there a standby arrangement to automatically pick up the system in case of primary failure?
b. What is the plan for dealing with a significant business interruption? How good is the service support system in such a case?
c. What types of interruptions does the business continuity plan cater for?
d. When last was the business continuity plan tested under normal operating conditions? Was the Audit Committee / Board briefed about the outcome(s) of tests carried out?
e. Which areas of the plan did not work as expected and what alternative plans were made?
f. Is the backup capacity sufficient?
g. What is the cost of providing for a parallel system?
h. How long will the recovery take and what will the cost to the organisation be?

i. Does the organisation have adequate IT-system specific insurance in cases of disaster and loss of information?

j. Is there confirmation of business continuity at least annually, either through Internal or External audit?

k. Is the Board / Audit Committee systematically and regularly briefed about the reliability and continuity of the adopted IT system?

5. Information security and privacy

a. How frequently does Management / the IT person brief the Audit Committee regarding network violations / security breach? Is the report duly documented?

b. When was the last occasion a network violation, however minor, was reported? Was the follow-up action brought to the attention of the Board / Audit Committee?

c. When was the last external penetration testing and internal vulnerability assessment made by a competent professional?

d. Is network violation becoming more recurrent? What was the nature of the last network violation? What was the impact of the last violation?

e. What measures were implemented to secure the network after the last violation? Was the nature of the intrusion duly investigated and were appropriate remedies applied against similar intrusion in the light of the information obtained?

f. Are there specific areas of activity more prone to unauthorised intrusions in the system? What has been done to secure such areas?

g. Has the organisation used outside providers to perform security testing and what has changed as a result?

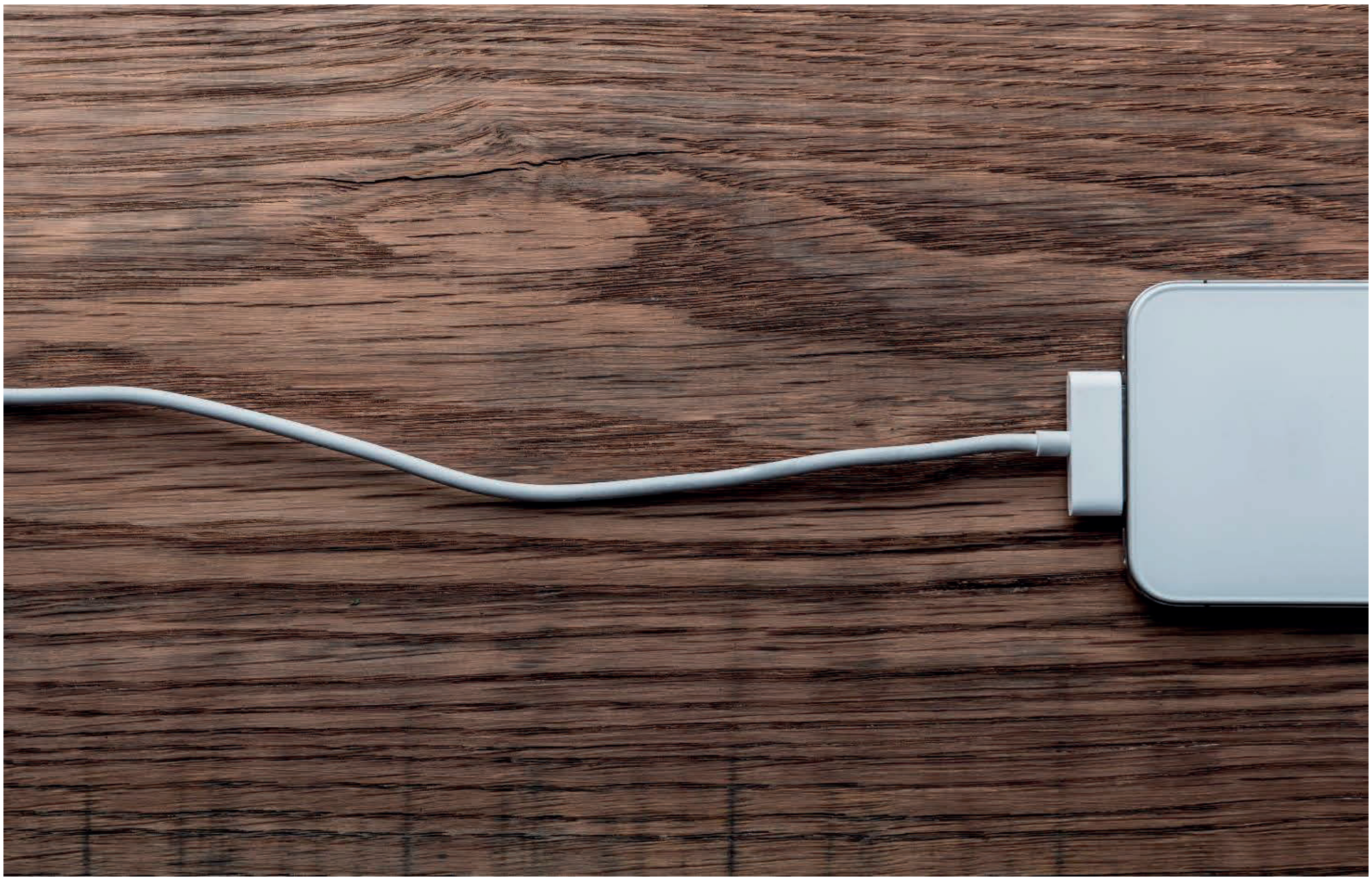
h. Do all electronic messages contain a disclaimer policy?

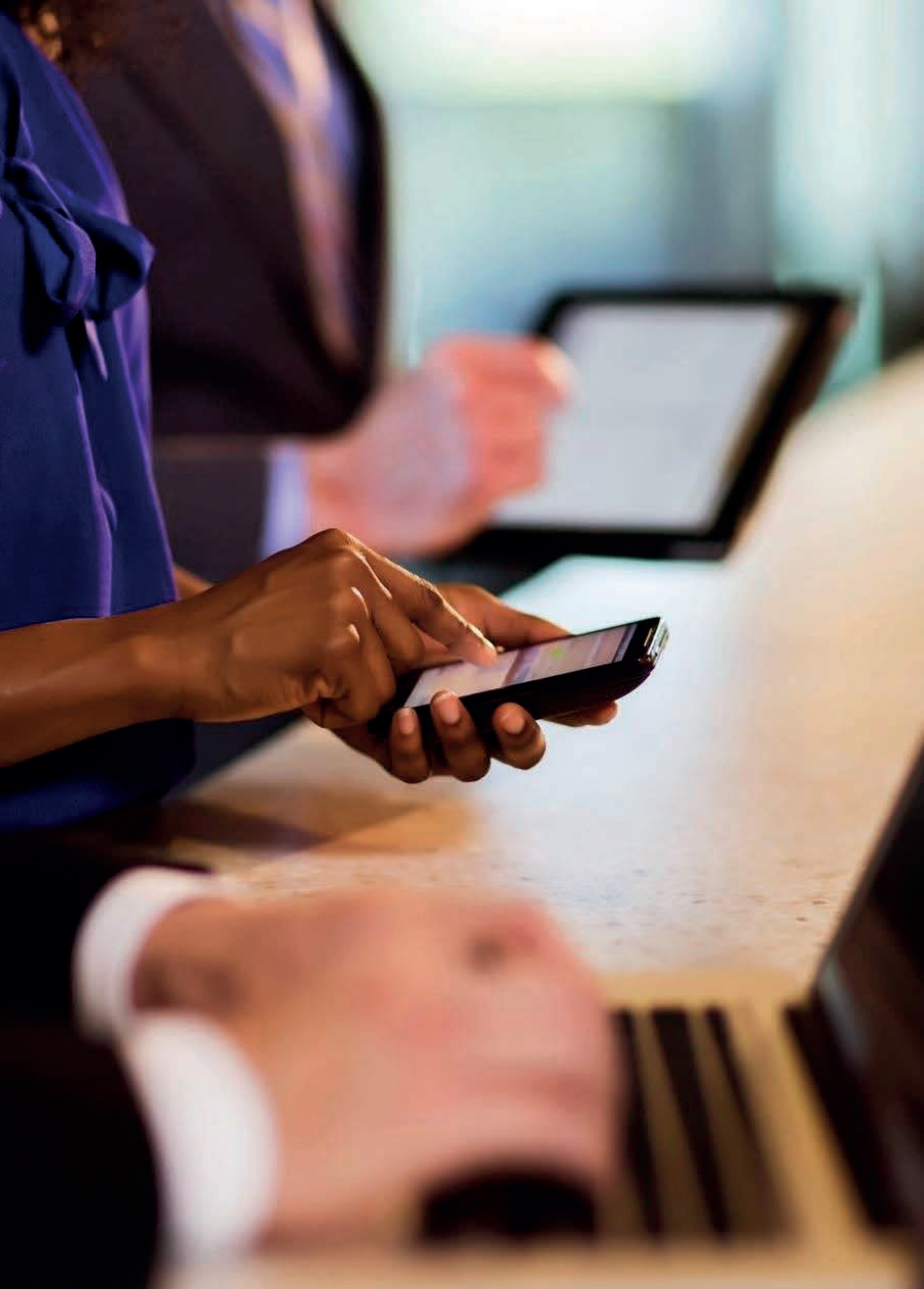
i. Has the organisation developed and communicated policies regarding the use of off-the-shelf software?

j. Is there appropriate and timely cleansing of data, prior to staff exiting?

k. Does the organisation abide by licensing agreements and are the agreements reviewed on a regular basis and confirmed independently?

l. How much critical information is derived directly from the system and how much rework is required?





KPMG

MIoD Mauritius Institute of Directors

Promoting Corporate Governance across the board

KPMG
KPMG Centre
31, Cybercity, Ebène, Mauritius
T: (230) 406 9999 **F:** (230) 406 9998
E: kpmg@kpmg.mu **W:** KPMG.com/mu
Business registration number: F07000189

Mauritius Institute of Directors
1st Floor, Standard Chartered Tower
19, Cybercity, Ebène, Mauritius
T: (230) 468 1015 **F:** (230) 468 1017
E: miod@miod.mu **W:** miod.mu
Business registration number: C08077130

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The KPMG name and logo are registered trademarks or trademarks of KPMG International.

The opinions of the authors are not necessarily the opinions of KPMG.