KPMG

MIoD Mauritius Institute of Directors
Promoting Corporate Governance across the board

Audit Committee Forum

Position Paper 10

Management of Cyber security risks in the new normal



October 2022

kpmg.com/mu

miod.mu

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 in Mauritius have set up the Audit Committee Forum (the Forum) in order to help Audit Committees in Mauritius, from both the public and the private sectors, improve their effectiveness.

The purpose of the Forum is to help Audit Committee members 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.

Position Paper 10 deals with management of cyber security risks in the new normal.

Previous Position Papers are listed at the bottom of this page* and may be consulted/downloaded from: https://home.kpmg.com/mu/ and http://www.miod.mu/

*Previous Position Papers

- Paper 1: Best Practice Guidance Notes for Audit Committees (July 2014)
- Paper 2: Interaction of Audit Committee with Internal and External Auditors (May 2015)
- Paper 3: The Audit Committee's Role in Control and Management of Risk (December 2015)
- Paper 4: Guidelines for the Audit Committee's assessment and response to the Risk of Fraud (October 2016)
- Paper 5: Guidelines for the Audit Committee's approach to Information Technology Risk (July 2017)
- Paper 6: Audit Committee Guidelines for evaluating whistleblowing systems (September 2018)
- Paper 7: Audit Committee Guidelines for the Evaluation of Retirement Obligations (August 2019)
- Paper 8: Guidelines for the Audit Committee on Data Protection (October 2020)
- Paper 9: Guidelines for the Audit Committee on Business Continuity (October 2021)

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.

Ujoodha Sheila – *Chairperson*
Aumeerally Feriel
Chung John
Cundasawmy Robin
Dinan Pierre
Gooroochurn Bharatee
Kee Mew Mervyn
King Antoine
Kistnamah Nagesh
Koenig Fabrice
Leung Shing Georges
Leung Steve
Molaye Sanjay
Mooroogen Sumita
Ong Su Lin
Ramdhonee Kalindee
Ramdin-Clark Madhavi

Secretary:
Bishundat Varsha

MIoD Coordinator:
Mulung Nafeeza



Contents

1. Introduction	**3**
2. Cyber security	**5**
3. Key Cyber security risks and safeguards	**7**
4. Role of the Audit Committee	**11**
5. Trends in the new normal	**15**
6. Conclusion	**17**
Appendices:	**19**
Appendix 1 – References	20
Appendix 2 – Glossary of terms	21
Appendix 3 – Ways to implement safeguards	22
Appendix 4 – Audit Committee Questions	25

Introduction



Technology is constantly changing, and this is transforming the digital ecosystem around the world including Mauritius. With rapid development in communication technology and the Internet of Things [IOT], the possibilities of connected devices have become endless. Embracing technology is a must for many organisations and due to the power of the Internet, there has been a growing number of businesses that do e-commerce and create other businesses online. Therefore, cyber security is a topical issue, and cyber risks can be considered as inherent risks for any organisation nowadays.

ACF Paper 9 on Business Continuity, has talked about cyber risks being among the top risks faced by organisations, and the needs for them to be prepared to address a cyber attack when it occurs; to enable the continuation of business. Also, with the introduction of EU GDPR in year 2019, and the revised Data Protection Act 2017 for Mauritius, organisations have become more conscious about protecting personal data over and above the usual concern regarding IT systems which are required to ensure confidentiality, integrity and availability of data, IT systems, and connectivity.

Addressing cyber security risks is surely a topic that needs to be on the Board's agenda. As per the National Code of Corporate Governance for Mauritius (2016), "*The Board should ensure that information assets be managed effectively, and should delegate to management the implementation of a framework on information, information technology and information security governance*". Thus the Board needs to ensure that the organisation has a robust system of internal technology controls, and where necessary, reinforce capacity at all levels to prevent cyber criminals from exploiting its weakest link in the organisation.

However, cyber security is above all everyone's responsibility, especially when using smart and/or mobile devices and technologies connected to the Internet. Who can live without technology in the 21st century; especially when digital systems are at the centre of every business and home? Working from home (WFH) or elsewhere, has become the new normal for many organisations following the pandemic of Covid-19, and WFH has undoubtedly increased the exposure to cyber attacks; including ransomware attacks and data breaches.

This position paper sets the tone on what Audit Committee members and the Board, including any person who oversees governance needs to know about cyber risk management. This will enable them to navigate the challenges while fully embracing technology, and being aware of the cyber risks and controls to be implemented to support resilience and achieve sustainable business growth.

KPMG

© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.



© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
Printed in Mauritius.

Cyber security

The National Institute of Standards and Technology (NIST) states that "*Cyber security threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the nation's security, economy, and public safety and health at risk. Similar to financial and reputational risks, cyber security risk affects a company's bottom line. It can drive up costs and affect revenue. It can harm an organisation's ability to innovate, and to gain and maintain customers. Cyber security can be an important and amplifying component of an organisation's overall risk management".*

Cyber security involves defending IT systems and infrastructure, including mobile devices, electronic systems, and data (and personal data) from malicious attacks. Previously referred to as IT security, which covers different areas such as network security, application security and information security; cyber security threats may be associated to these three key elements:

- Cybercrime - includes mainly targeting systems for financial gain or to cause disruption.
- Cyber attack - mainly involves stealing of confidential/sensitive information e.g. personal data.
- Cyber terrorism - mainly attacking electronic systems to cause panic or fear.

A few statistics from IBM's Cost of a Data Breach Report 2021 following a survey carried out across 17 countries and regions, and 17 different industries are:

- Data breach costs have increased by 10% (from USD 3.86 million to USD 4.24 million) from 2020 to 2021, being the highest average total cost in 17 years.
- The top five industries with the highest average total cost were Healthcare (USD 9.23 million), Financial (USD 5.72 million), Pharmaceuticals (USD 5.04 million), Technology (USD 4.88 million), and Energy (USD 4.65 million).
- Business email compromise was responsible for only 4% of breaches at USD 5.01 million. The second costliest was phishing (USD 4.65 million), followed by malicious insiders (USD 4.61 million), social engineering (USD 4.47 million), and compromised credentials (USD 4.37 million).
- The most common initial attack vector was compromised credentials accounting for 20% of breaches, followed by phishing attempts (17%), and cloud misconfiguration (15%).

According to the Global Security Outlook 2022, the cost of breaches to an organisation is high, amounting to an average of USD 3.60 million per incident and that companies need 280 days on average to identify and respond to a cyber attack. Cyber leaders from 20 countries are most personally concerned about the following top three types of attacks:

1. Infrastructure breakdown due to a cyber attack;
2. Identify theft; and
3. Ransomware.

KPMG

© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

However, can we say that organisations in Mauritius are sufficiently protected against cyber threats and attacks? And to what extent can we trust technology nowadays? As per the Global Cyber security Index (GCI) 2020 published by the International Telecommunication Union (ITU), Mauritius is ranked 17th globally and 1st in the Africa region regarding cyber security. With the rapid evolution in technology, the threat landscape for an organisation is evolving, and the way a business operates has to change.

In 2021, the Mauritian Government enacted the Cyber security and Cybercrime Act 2021 and as per this Act, a National Cyber security Committee will be setup in Mauritius to discuss on cyber security matters facing both public and private organisations and provide recommendations.

Previously, in August 2019, the Financial Services Commission (FSC) in Mauritius issued specific guidelines to companies on cyber security risk governance requiring regulated entities to:

- understand cyber risks, vulnerabilities and impact associated in running their businesses, with supporting documentation;
- put into place appropriate policies and procedures approved by the Board to mitigate the risks;
- carry out an annual cyber security risk assessment which is reported to the Board;
- conduct regular IT audit and addressing identified loopholes accordingly;
- conduct penetration tests to ensure that their systems are not vulnerable or susceptible to cyber attacks;
- put in place appropriate contingency arrangements that can be deployed in the event of a cyber attack, including but not limited, maintaining service levels for clients, and informing relevant parties and authorities about the attack and its impact; and
- run a comprehensive technology risk and cyber security training programme at all levels.

A lot of guidelines and papers cover IT security, cyber security and governance e.g., ISO 27000 series, COBIT 2019, and NIST Cyber security Framework. These resources can help organisations secure their technology environment, and be better prepared to face cyber threats. Currently, the Mauritian public can report cybercrimes occurring on social media securely through the Mauritian Cybercrime Online Reporting System (MAUCORS) which is a national online system administered by the Computer Emergency Response Team of Mauritius (CERT-MU).

The CERT-MU's responsibility is to provide technical assistance to law enforcement regarding cybercrime.

Statistics of Cyber security attacks in Mauritius

For the period from 2018 to June 2022:

- Total No. of incidents reported to CERT-MU on MAUCORS: 7,838

The type of offences reported consists of the following:

- Hacking
- Online harassment
- Offensive content
- Sextortion
- Identity theft
- Cyber bullying
- Cyber stalking
- Scam and fraud
- Phishing
- Malware

© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

Key Cyber security risks and safeguards

Cyber security problems can range from things as granular as out-of-date software to large-scale struggles like a lack of support from leadership teams.

Examples of the most common issues facing information security professionals, and the organisations they serve include:

1 Recognising that you are a target

Small organisations don't always realize that their assets and data are attractive to cyber criminals. Organisations of every size face cyber threats. It means being constantly aware that you are a target. The majority of breaches occur because of human error. Acknowledging that attackers might target your organisation is step number one to developing a defence.

2 Failure to inform employees of threats

The weakest link in any cyber security program is often the employees. A huge amount of money can be spent on antivirus, intrusion detection, next-generation filters and other technologies, but the effectiveness of such technology will be limited if staff are not educated.

Organisations should think of their employees as the first line of defence when it comes to basic threats like phishing and malware.

Identify your most at-risk users and empower them with the knowledge and awareness to identify these scams. This may have been many people's first time working from home. Many simply do not know how to stay safe and prevent cyber attacks like ransomware. They don't have someone next to them at the office to ask if the emails are legitimate, or if a website looks safe to download a file from.

3 Data breaches due to remote work

With more people working from home and other locations outside the office, there is a greater chance of breaches from hackers. Connections to other networks, with non-approved devices, can happen in these situations.

4 Ransomware attacks

Ransomware is a type of malware that can encrypt files on a device, making them inaccessible or unusable. Once the files are corrupted, the attackers then demand a "ransom" in exchange for decryption. Attackers also threaten to expose or sell stolen information should the ransom, which is usually demanded in cryptocurrency, not be paid. The demands are often preceded by phishing attacks to steal credentials. As organisations become more aware of the need to secure their data backups, ransomware threat actors are focusing more on the data breach extortion methods to pressurise their victims into paying the ransoms.

5 Missing security patches

Delaying the installation of new security patches puts organisations' assets at risk.

KPMG

© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

6 Bring Your Own Device (BYOD) threats

Again, the disruption caused by COVID-19 has intensified the security issues in BYOD threats. Bring your own device policies are popular in many companies. BYOD lets employees use their own machines for work in office or remotely, to make things easier.

But many business leaders don't appreciate the unique threats that a BYOD environment can invite into their organisations.

7 Losing sight of the 'backup plan'

Most organisations do not see backups as part of their cyber security initiative. Without the ability to decrypt, and without backups, the data is gone forever. Incremental offsite backups are so important, yet often overlooked.

8 Lack of a corporate security program

One surprisingly prevalent security issue faced by organisations, is their lack of a formal corporate security program. Every organisation, no matter the size, should have a security policy outlining acceptable use, incident response, physical security, and at least a dozen more areas.

This proactive approach to cyber security is the missing ingredient in many businesses.

9 Treating cyber security like an IT issue instead of a financial issue

Many business leaders still treat cyber security like an IT issue, when it really is about the bottom line. Cyber security attacks, at their core, are a financial issue.

In essence, it is a business risk mitigation exercise that requires strategic thinking and ongoing tactical actions.

10 Lack of information security representation on the Board

Many business leaders still treat cyber security like an IT issue, when it really is about the bottom line. Cyber security attacks, at their core, are a financial issue.

In essence, it is a business risk mitigation exercise that requires strategic thinking and ongoing tactical actions.

11 Sniffing attack

Sniffing attack in context of network security, corresponds to theft or interception of data by capturing the network traffic using a packet sniffer (an application aimed at capturing network packets). When data is transmitted across networks, if the data packets are not encrypted, the data within the network packet can be read using a sniffer.

KPMG

© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

Human error

Human error is the main cause of 95% of cyber security breaches, which encompass unintentional actions as well as a lack of the appropriate action. The mitigation for these errors can come from two perspectives: reducing opportunity and educating users.

While untrained end-users may be the weakest link the security of an organisation, the right tools and training allows to empower them into the first line of defence against any attack or breach, safeguarding the business in the long term.



Safeguards

Safeguards are protective measures and controls prescribed to meet the security requirements specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Here are some examples:

1. Lead from the front. Ensure the Board understands and strategise for cyber resilience
2. Encrypt data at rest and create resilient back-ups
3. Conduct regular employee training and test your incident response plans
4. Keep systems and software fully updated
5. Implement Multi-Factor Authentication during a transition from passwords to passkeys
6. Assess and monitor vendors
7. Reduce your attack surface through systems harmonisation
8. Pay close attention to physical security and integrate it with digital security
9. Ensure incident response plan includes the ability to isolate networks and systems
10. Install smart firewalls and integrated monitoring with endpoint security

For more details, please refer to Appendix 3.

© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.



© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
Printed in Mauritius.

Role of the Audit Committee



Why should Cyber security risks be a continuous Board concern?

The threat landscape is expanding. Cybercriminals, internal and external, are as entrepreneurial as ever, and using increasingly sophisticated tools and technologies to seek out vulnerabilities in the platforms used, to then carry out cyber attacks.

While internet increases the connectivity and efficiency of organisations, it also brings numerous threats, such as cyber hacking and online attacks, which result in financial loss, disruption or damage to the reputation of an organisation from failure, unauthorised or erroneous use of its information systems.

Since the last two decades, organisations are being faced with cyber security risks, particularly phishing, identity fraud and email compromise, as one of the fastest-growing threats to their data and financial success today. As technology advances and changes, cybercriminals are using it to compromise and steal business assets.

Additionally, internal errors like misconfigured servers, or employees who accidentally leave data open to the Internet, along with cyber risks, expose an organisation to many threats: from theft to reputational loss.

In such a fluid environment as above, IT security should be a strategic concern of the Board which must ensure adequate communication between the Cyber security team and the organisation, to ascertain appropriate level of awareness in respect of the associated risks. Furthermore, consideration should be given to the appointment of a person with information technology background on the Board.

The Board of small organisations should be aware whilst cyber attacks target everyone, trends show small businesses are one of the most common targets. In fact, according to Verizon's 2021 Data Breach Investigation Report, 46% of breaches impacted small and midsize businesses. However, there are effective software and online security measures which can be put in place to help protect organisations from cybercriminals.

KPMG

© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

What are the Board's responsibilities?

The Board should ensure that the following key cyber security concerns are fully addressed:

- Expanding the strategic security conversation: Change it from cost and speed to effective security to help deliver enhanced business value and user experience to align business goals with security needs.
- Achieving the organisation's X-factor: Use critical talent and skillsets to transform the cyber security officer or team from enforcer to influencer.
- Adapting cyber security for the cloud**:** Enhance cloud security through automation, from deployment and monitoring to remediation.
- Placing identity at the heart of zero trust: Adopt Identity and Asset Management (IAM) and zero trust in today's hyperconnected workplace.
- Protecting the privacy frontier: Move to a multidisciplinary approach to risk management that embeds privacy and security by design.
- Securing beyond the boundaries: Transform supply chain security procedures from manual and time-consuming to automated and collaborative.
- Reframing the cyber resilience conversation: Broaden the sustainability of operations to manage the consequences when a cyber attack occurs and enable rapid recovery.
- Exploiting Cyber security automation: Use smart deployment of security automation and artificial intelligence to help realise added value to the organisation.

The Board should also ensure that employees receive security awareness training and learn about the best practices to prevent and mitigate the cyber security risks and threats and the protection and safeguards provided under the Cyber security and Cybercrime Act 2021.

Preparedness / readiness of the Board

A significant reason why cybercrime and breaches are rising is that most people just view them as someone else's problem. However, safeguarding our digital identities and data is an individual, and global concern.

The last two pandemic years have redefined how organisations operate, govern and conduct their businesses. Securing and protecting critical assets, systems and, most importantly, sensitive proprietary and customer data, is no longer exclusively an issue for security and IT professionals. Rather, handling and mitigating risks to help the strategic viability and operational sustainability of the entire business, is a shared responsibility within the whole business; with the tone to be set at the top.

The Audit Committee will be of great help and support to elevate boardroom visibility. Digital technology now powers and empowers organisations, much like electricity did during the industrial revolution. It also has the ability, if insufficiently secured or resilient, to interrupt communications and disrupt supply chains. A single data breach or malware attack has the insidious capacity to incapacitate real-time transactions and network interactions, and ultimately disrupt business and impact revenue growth for days, if not weeks and months.

Trust is becoming a defining theme nowadays, and effective cyber security implementation can play a vital and fundamental role in further building that trust in a digital world, and enable a business to gain a competitive advantage.

KPMG

© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

The following key strategies should form the foundation of any cyber security program to be adequately resilient to modern cyber threats in the new normal. They are also considered as essential to enable the Board to easily make a self-assessment of the effective implementation of the organisation's cyber risk management strategy.

- Responsibility: To assert the organisation's ownership of cyber risk management, the Board should appoint a ''Cyber Risk Champion'", preferably a non-technical specialist, who would be responsible for the oversight of cyber risk management.
- Information asset awareness: maintaining a register for all asset data, sorted both by category and criticality, with a description of each type of asset, where stored and processed, as well as the assigned owner who can assign appropriate access.
- Payment control: Almost all cybercrimes are focussed on fraud. Strict payment controls, such as segregation of duties, should be in place for the payment systems which are now online for many businesses. Arrangements in place should include not only finance staff but extend to staff in procurement and audit as well.
- Budget: It is vitally important that the budget for IT and cyber security be adequate. An effective way to do this is to express it as an average percentage of revenue. Budget should include IT staff remuneration, third party costs including subscriptions, maintenance of existing IT and procurement of new systems.
- IT and cyber security staff count ratio: This ratio to end-users needs to be closely monitored and, for outsourced services, the yardstick would be the number of IT staff equivalence that would have been insourced to provide the required services. Furthermore, the IT Department should be given proper prominence within the organisation.
- Skills and staff awareness: Sufficient investment is a necessity in the training of the IT staff and skills acquisitions, to guard the organisation against security problems before they occur, a pre-requisite for career growth and/or job performance. All staff should be given awareness training to enable them to spot cyber incidents and scams.
- Technology versions: The technology platform used by the organisation should be aligned with the NIST framework and be procured from a supplier supporting the latest technology version which is to be maintained so as to keep ahead of cyber attackers.



KPMG

© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.



An emerging trend, amongst the top risks

The most successful organisations not only treat cyber security as key to their future success but also look to engender client and customer trust in their cyber resilience, in their protection of sensitive data, and in the transparency of their approach.

Cyber security threats have been on the rise, with the Covid-19 having a big impact and boosted cyber security among the top risks facing any organisation. The progress of digital transformations has inevitably led to new cyber security threats. Cybercriminals take advantage of the Covid-19 pandemic, in particular by targeting businesses working remotely. During the pandemic, organisations had to quickly adapt to new working conditions and thus opened new doors and more possibilities for cybercriminals.

The extent of the Audit Committee's involvement in cyber security issues varies significantly by company and industry. In some organisations, cyber security risk is tasked directly to the Audit Committee, while in others, there is a separate risk committee.

Companies for which technology forms the backbone of their business often have a dedicated cyber risk committee that focuses exclusively on cyber security.

Regardless of the formal structure adopted, the rapid pace of technology and data growth, and the attendant risks highlighted by recent security breaches demonstrate an increasing importance in understanding cyber security as a substantive, enterprise-wide business risk.

Audit Committees should be aware of cyber security trends, regulatory developments and major threats to the company, as the risks associated with intrusions can be severe, and pose systemic economic and business consequences that can significantly affect shareholders. Engaging in regular dialogue with technology-focused organisational leaders will help the Audit Committee better understand where attention should be concentrated. Some questions for Audit Committees to consider asking management regarding cyber security are listed in Appendix 4.

KPMG

© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

Trends in the new normal

Since the start of the pandemic, many organisations have broken digital barriers at record speed. The era of cloud computing, Internet of things, artificial intelligence and online collaboration tools has accelerated digital automation and human connectivity. But these new hybrid human-digital ecosystems are often fragile. And threats are increasingly sophisticated. To outrun emerging cyber threats, organisations will need to think creatively to create a holistic team of cyber defenders with the capabilities to stay ahead of the criminals.

Digitisation trends have left many cyber security professionals and organisations on uneven ground. These challenges often run deep, and have been gaining momentum since before the current Great Resignation and start of Covid-19. Cloud security, security awareness, endpoint security, and real-time threat intelligence capabilities are top priorities.

Organisations cannot afford to wait for fresh talent to come in. Cyber security is still a relatively new field of study on college campuses, and threats and strategies for managing them are ever-changing. To prepare both new and experienced talent, organisations should understand skill gaps and move employees through cyber security upskilling quickly without sacrificing skills acquisition.

Skills diversity

Cyber professionals in general should continue to evolve their skills in a more system-based, strategic business direction. As an industry, cyber teams should not only seek to attract more talent in an absolute sense but be open to a broader range of diversity of talents.

Cyber security faces a critical skills gap across a wide range of areas, including cloud security, operational technology security, data science and analytics, security architecture and engineering, and attack simulation.

The trend for cyber security generalists appears to have declined, with a new demand for and appreciation of people with strong technical capabilities. Organisations now realise the importance of both leadership and technical skills in cyber security teams.

Looking further ahead, new roles are evolving that may not even exist today, such as resilience strategist, cyber risk modeler, orchestration manager, behavioural analyst, and artificial intelligence ethicist. Vendor management has also taken on greater relevance, with the surge in outsourcing and third-party partnerships — especially for cloud-based services, where cyber teams must share responsibility for security. In shaping the future cyber security workforce, Chief Information Security Officers (CISOs) will have to consider how to access both existing and new capabilities needed to stay on top of emerging threats, rebalancing the skills within their organisations to meet the changing demands.

Key attributes sought in cyber security personnel:

- Strong problem-solving abilities
- Curiosity / eager to learn
- Cyber security certifications
- Strong communication skills
- Relevant cyber security work experience
- Relevant IT work experience
- Knowledge of basic cyber security concepts
- Knowledge of advanced cyber security concepts
- Strong strategic thinking skills
- Cyber security qualifications other than certifications or a degree

[Source: —(ISC) Cyber security Workforce Study, 2021]

KPMG

© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

The growing importance of a broader mix of skills, both technical and non-technical, underscores the reality that cyber security roles are multi-dimensional and increasingly varied across specialisations, organisations and industries

Outsourcing of skills

To shape a dynamic 21st century workforce, CISOs must constantly assess what capabilities are needed, and then source these skills from within and outside the organisation — using a hybrid model of permanent hires, temporary workers and contract models.

Increasingly, we are likely to see CISOs outsource some of their operations. This may be to specialist providers that can scale up and down at ease; professional services companies offering transformation support and strategic advice; and niche service providers and contractors. And, as organisations continue to migrate to the cloud, they will look to cloud service providers for a growing range of security activities.

A key question for CISOs will be 'What skills do they need to retain in-house?', to establish a core team that lets the organisation govern its security, set strategic direction, make tough and informed choices on risk, and manage incidents and crises. Beyond this core will be a complex tapestry of sourcing strategies and relationships with outsourced and co-sourced suppliers, who provide the scale and specialist skills needed for security operations, as part of the shift to a shared responsibility model. Increasing regulatory expectations around the role and competence of CISOs and their teams will also impact on roles and responsibilities.

When sourcing external cyber security skills, care must be taken to ensure that providers are not conflicted in the provision of security, as opposed to other IT services. For example, those responsible for regular security monitoring should not also be tasked to investigate breaches.

Cyber liability insurance

The ever-evolving cyber risk landscape is driving interests in cyber liability insurance as one complementary element to transfer some of the risks associated with cyber incidents to their insurance provider. Cyber liability insurance covers financial losses resulting from data breaches and other cyber events such as network intrusions, phishing attacks, ransomware, etc. The insurance covers areas such as loss or theft of data; privacy breach, business interruption, cyber extortion, crisis management costs amongst others.



© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

Conclusion

Cyber risk has become a buzzword in recent times, as the world relies more and more on digital information and IT-driven business processes. Beyond this, lie serious business implications if words are not put into action. The importance of adequate governance structures, risk management practices, and compliance oversight cannot be underestimated, if an organisation seeks to withstand the tests of the digital age. The topic of cyber security must feature on the Board's agenda and executives are expected to treat cyber risk as an operational risk.

Digital infrastructure supports almost every aspect of our lives, from healthcare and banking to energy. Cyber attacks can therefore have catastrophic consequences for businesses, governments and citizens. Despite the headlines seen over the past two years indicating a dire need for better protection against cyber attacks, there is still a cyber security workforce gap of more than 2.72 million positions. While that number has been steadily decreasing year after year, it's simply not enough. According to the 2021 (ISC)² Cyber security Workforce Study, the global cyber security workforce needs to grow by 65% to effectively defend organisations' critical assets.

As our mental and physical wellbeing depend more greatly on the digital world, cyber security professionals should be considered as essential as any other protector of our lives.

There is an urgent need to close the current cyber security skills gap to ensure critical assets are protected.

A cyber resilient organisation understands that things will go wrong, and cyber security breaches will occur. In such an eventuality, reliable and trustworthy people are needed with deep technical knowledge and experience for complex investigations.

Cyber security is no longer be considered as merely a technical issue, after having spilled over to the geopolitical realm. Critical technologies have transformed to englobe basic digital technologies, and communications infrastructure, and emergent ones such as 5G, cloud computing, artificial intelligence, and quantum computing. The associated cyber risks are conduits to impact a country's national security, economic progress, and societal values. Cyber capabilities and critical technologies are shaping up as tools of state power that can be used against adversaries.

Most importantly, the Board executives must properly understand, and implement strategies which fully support the tactical and operational activities of effective cyber risk management. Failure to do this will leave their organisations highly exposed to critical incidents which increasingly are bringing businesses of all types and sizes to their knees.



KPMG

© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.



© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
Printed in Mauritius.

Appendices



© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
Printed in Mauritius.

Appendix 1
References

References

- Financial Services Commission Mauritius, 2019, Circular Letter (CL210819) on “Re: Cyber Security Risk Governance”.
- Government Gazette of Mauritius, No.173, 2021, Cyber security and Cybercrime Act 2021.
- IBM Corporation, 2021, Cost of a Data Breach Report 2021.
- International Telecommunication Union (ITU), 2021, Global Cyber security Index (GCI) 2020
- KPMG, 2021, Audit Committee Forum Position Paper 9: Guidelines for the Audit Committee on Business Continuity.
- The Ministry of Financial Services, Good Governance and Institutional Reforms, 2nd edition 2016, The National Code of Corporate Governance for Mauritius (2016).
- World Economic Forum, 2022, Global Security Outlook 2022.
- (ISC)² Cyber security Workforce Study, 2021.

Useful Websites:

- http://cyber security.ncb.mu/English/Pages/default.aspx
- https://govmu.org/EN/infoservices/comm/Pages/security.aspx
- https://maucors.govmu.org/maucors/

KPMG

© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

Appendix 2
Glossary of terms

BYOD (Bring Your Own Device) — A company's security policy dictates whether or not workers can bring in their own devices into the work environment, whether or not such devices can be connected to the network; and to what extent that connection allows interaction with company resources. A BYOD policy can range from complete prohibition of personal devices being brought into the facility to allowing any device to be connected to the company network with full access to all company resources.

Critical infrastructure — The physical or virtual systems and assets that are vital to an organisation or country. If these systems are compromised, the result would be catastrophic.

Cryptojacking — a type of cybercrime where a criminal secretly uses a victim's computing power to generate cryptocurrency. This usually occurs when the victim unwittingly installs a programme with malicious scripts which allow the cybercriminal to access their computer or other Internet-connected device, for example by clicking on an unknown link in an e-mail or visiting an infected website.

Cyber attack — Any attempt to violate the security perimeter of a logical environment. An attack can focus on gathering information, damaging business processes, exploiting flaws, monitoring targets, interrupting business tasks, extracting value, causing damage to logical or physical assets or using system resources to support attacks against other targets.

Cyber security — The efforts to design, implement, and maintain security for an organisation's network, which is connected to the Internet. It is a combination of logical/technical, physical and personnel focused countermeasures, safeguards and security controls.

Cyber teams — Groups of professional or amateur penetration testing specialists who are tasked with evaluating and potentially improving the security stance of an organisation.

Encode/encrypt — The act which transforms plaintext or cleartext (i.e. the original form of normal standard data) into ciphertext (i.e. the unintelligible and seeming random form of data that is produced by the cryptographic function of encryption).

Firewall — A security tool, which may be a hardware or software solution that is used to filter network traffic. A firewall is based on an implicit deny stance where all traffic is blocked by default.

Hacker — A person who has knowledge and skill in analysing program code or a computer system, modifying its functions or operations and altering its abilities and capabilities.

Internet of things (IoT) - A system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

Malware (malicious software) — Any code written for the specific purpose of causing harm, disclosing information or otherwise violating the security or stability of a system. Malware includes a wide range of types of malicious programs including: virus, worm, trojan horse, logic bomb, backdoor, Remote Access Trojan (RAT), rootkit, ransomware and spyware/adware.

Phishing — A social engineering attack that attempts to collect information from victims. Phishing attacks can take place over e-mail, text messages, through social networks or via smart phone apps.

Ransomware — A form of malware that holds a victim's data hostage on his computer typically through robust encryption. This is followed by a demand for payment in the form of Bitcoin (an untraceable digital currency) in order to release control of the captured data back to the user.

Social engineering — An attack focussing on people rather than technology. This type of attack is psychological and aims to either gain access to information or to a logical or physical environment. A social engineering attack may be used to gain access to a facility by tricking an employee into assisting by holding the door when making a delivery, gaining access into a network by tricking a user into revealing their account credentials to the false technical support staff, or gaining copies of data files by encouraging an employee to cut-and-paste confidential materials into an e-mail or social networking post.

Vulnerability — Any weakness in an asset or security protection which would allow for a threat to cause harm. It may be a flaw in coding, a mistake in configuration, a limitation of scope or capability, an error in architecture, design, or logic or a clever abuse of valid systems and their functions.

KPMG

© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

Appendix 3
Ways to implement safeguards

1. Encrypt data and create backups

Make sure all sensitive data is encrypted. Saving data in normal-text format only makes it easy for hackers to access. Data encryption, on the other hand, limits data access to parties that have the encryption key. Some data encryption software raise notifications when other people try to alter or tamper with the information.

Regular backups should be conducted for important information. Cyber security breaches can sometimes result in data loss. When this happens, and there is no reliable and secure backup available, it could result in operational disruptions that might cause the organisation a large revenue loss.

2. Conduct regular employee training

One of the common ways malicious hackers gain access to an organisation's database is through phishing emails sent to employees. In fact, statistics show that over 3.4 billion phishing emails are sent globally. These emails contain malicious malware in the form of links that give hackers access to user data, including login credentials.

Phishing emails are often hard to detect as they seem legitimate. For instance, a hacker may send an email impersonating leaders in the organisation, asking for personal details. Without proper training, the employee may end up divulging this information. That is why it is vital to conduct cyber security awareness training. Employees need to be informed of the main forms of cyber security attacks, and the best ways to prevent them.

3. Keep systems and software updated

Software and system updates highly impact an organisation's cyber security and digital safety. This is because they not only add new features but also fix bugs and help patch security flaws and vulnerabilities that can be exploited.

Malicious hackers write code that they use to exploit these vulnerabilities. Most of the time, this code is packaged in the form of malware which can affect an organisation's entire system. So, make sure a patch management system is used to automatically manage all updates and uphold information security.

4. Use of strong passwords

Over 80% of organisational data breaches result from weak passwords. Hackers do not require much information to gain access to an organisation's systems. They will fully exploit a small gap until they are into the system.

Password cracking technology has greatly advanced, and simple passwords don't cut it anymore. Instead, use of complex passwords should be made compulsory, and multi-factor authentication strategies should be deployed to discourage cyber crime in an organisation. Password sharing among employees should be discouraged so that even if one desktop is hacked, the rest remain secure. Password should be kept safely in an encrypted format.

With many employees now working from home, bring-your-own-device (BYOD) is becoming increasingly common. Make sure these devices have strong passwords and are scanned for viruses and malware before connecting to the office network.

5. Assess and monitor the vendors

Chances are that an organisation's cyber security is highly dependent on third-party vendors, which means that vendor risk management cannot be ignored. This would help to mitigate third-party risk instead of solely relying on incident response.

The main focus should be on:

- Cyber security risk: onboard vendors using the right strategies and monitor them.
- Legal, regulatory, and compliance risk: ascertain that the vendor will not impact the organisation's compliance with regulations, agreements, and local legislation.
- Operational risk: if the vendor is a critical aspect of the organisation, ensure that they won't disrupt the operations.
- Strategic risk: ensure the vendor will not impact the organisation's ability to meet its objectives.

KPMG

© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

6. Reduce attack surface

Attack surfaces are the vulnerabilities or entry points that malicious hackers can use to access sensitive data. These could be anything like IoT, software, web application systems, and even employees that are often susceptible to social engineering attacks such as whaling and phishing.

There are 3 main types of attack surfaces:

1. Physical attack surface: this includes organisational assets that a hacker can get if they have physical access to its premises.
2. Digital attack surface: these are assets that are accessible through the internet and live outside a firewall. Digital attack surfaces include known assets such as the corporate servers/ operating system, unknown assets such as a forgotten website, and rogue assets such as apps that impersonate the organisation.
3. Social engineering attack surface: this is one of the most critical yet often overlooked attack surfaces. In this case, the hackers exploit human psychology and manipulate an organisation's employees into divulging sensitive information.

An organization should conduct an attack surface analysis to determine its threat landscape, identify all security gaps and reduce the attack vectors.

7. Pay close attention to physical security

Most organisational cyber risk management policies focus on the digital aspect of cyber risks and entirely neglect their physical premises. Conduct a security assessment and determine whether the critical infrastructure is safe from security breaches.

Sometimes online systems might be safe from cybercriminals, but a breach can still be possible through physical entry into the organisation's premises and access to its file cabinets. That would be tragic! There are even other instances where janitors go through the garbage, and obtain customer and employee personal information.

Restricted areas in an organization should be protected using high-value systems. A 2-factor authentication such as keycards and biometrics should be used. This way, even if the keycard is lost or stolen, no one will be able to access the area.

8. Put a killswitch in place

Having a killswitch protects an organisation from large-scale attacks. It is a form of reactive cyber security protection strategy where the information technology department shuts down all systems as soon as they detect anything suspicious until the issues are resolved.

Most of the time, cybercriminals don't cover their tracks, especially when they don't expect to be caught. So, IT security teams should analyse all server logs frequently and conduct cyber security framework audits to make sure their integrity is intact. Investment should be made in network forensic analysis tools that analyse information flow through the network.

9. Install firewalls

Cyber security threats are becoming more sophisticated, and everyday hackers come up with new ways of accessing data. Networks can be defended from cyber attacks by installing firewalls. A reliable system will effectively protect the organisation from brute attacks or prevent security incidents from causing irreversible damage.

In addition to this, firewalls monitor the network traffic to identify any suspicious activity that could compromise data integrity. They also prevent complex spyware from gaining access to an organisation's systems and promote data privacy.



© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

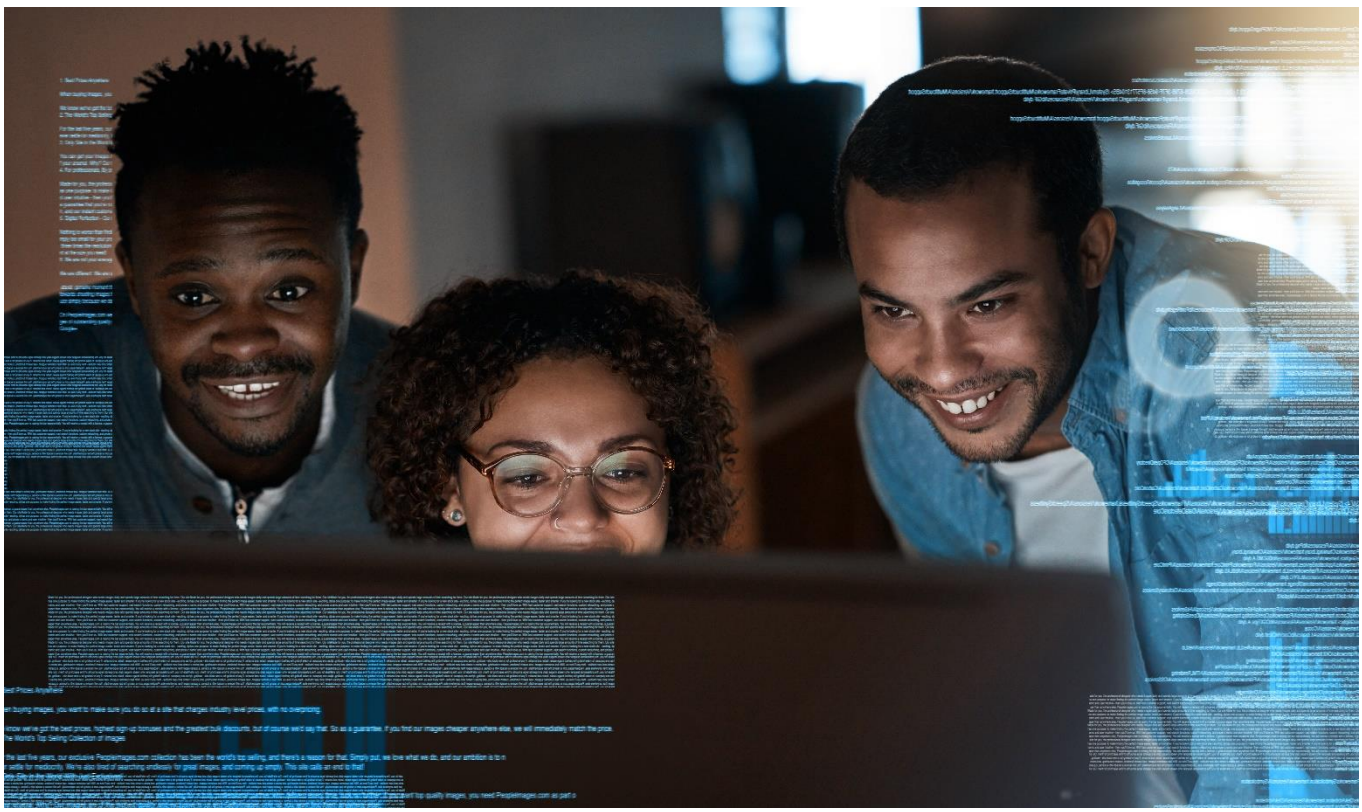
10. Create a secure cyber security policy

The organisation's cyber security is highly influenced by the policies that it has in place. Are there guidelines for data breach prevention and detection? How often do the IT teams conduct risk assessments or penetration testing? It all starts with the organisation's guidelines.

Existing policies should be reviewed, and any loopholes identified. Some of the guidelines that should be considered are:

- Disaster recovery: If a breach occurs, a disaster recovery plan ensures that the employees and IT teams know the next course of action. It's aimed at reducing the amount of downtime, thereby ensuring that your operations resume as soon as possible.
- Access control/management: this policy highlights the parties that can access sensitive information, reducing the risk of unauthorised access. Data mishandling has both financial and legal consequences.
- Security testing: the policy should state the frequency of cyber security tests. This allows to uncover vulnerabilities before it's too late. Some of the security tests that should be conducted include: vulnerability scanning, security posture assessment, penetration testing, ethical hacking, cyber security assessments, etc.
- Incident response plan: this is documentation of the steps and procedures that should be implemented in case of a breach. It also highlights the responsibility of key information security players and reduces the organisation's response time.

The organisation's cyber security policy should include a clause that highlights the consequences of data mishandling as well as the legal steps that will be taken on employees that are the cause of a breach. This will discourage insider attacks.



© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

Appendix 4
Questions for Audit Committee

Some questions that Audit Committees can ask management regarding Cyber security are:

Information and cyber security foundations

- Is the organisation 'cyber ready' at all times, or is there increased Board and management scrutiny on information and cyber security only when there is a publicised security incident?
- Does the organisation have a specific suitably qualified senior person responsible for information and cyber security? Does the organisation have a specific department handling cyber security?
- Is there an integrated three lines of defence approach to assurance activities over information and cyber security?
- Are there up-to-date policy and procedures in place that provide an effective framework for information and cyber security?
- Does the organisation have a 'hotline' to report cyber security incidents?
- Is there a defined and controlled policy for IT procurement? Does the organisation dispose of old and obsolete IT assets in a secure and timely manner?



Risk and threat assessment

- Does the organisation's enterprise risk management include cyber threats and monitoring procedures?
- Does the organisation have a clear understanding of what the cyber security risks are?
- Has the organisation applied a risk-based approach to identify its most important IT assets and what it needs to protect? Does this include (a) infrastructure (b) hardware (c) network (d) software (e) specific data?
- Has a cyber security threat risk assessment been performed? Have improvements been identified and a risk-based triage approach taken to implementation? Are responsibilities for implementation assigned, actively tracked and reported upward to the top level of the organisation including the Board?
- Has the CIO and Board thought on possible attacks:

i. Who might attack?

ii. What are they after, and what business risks do the organisation need to mitigate?

iii. What tactics might they use?

iv. How robust are the organisation's incident response and communication plans?

v. Are controls in place to guard against known and emerging threats?

vi. Can we detect malicious or unauthorised activity, including the unknown?

vii. Can we act and recover quickly to reduce impact?

KPMG

© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

IT access

- Is there an IT user privileges matrix built around specific job roles? Is this regularly reviewed to provide assurance that the privileges that people have are the ones they need to do their job? Is there a process to immediately revoke out-of-date privileges?
- Is there layered security measures and effective controls over employee remote access to the organisation's IT environment? Is access limited to use of organisation's IT assets only, and not personal and home computing for work purposes?
- Have information and cyber security policy and procedures been effectively disseminated and people trained in their use? Does this include staff, management, contractors and consultants? Does this include initial training and regular refresher training?

Disaster recovery

- Is information and cyber security covered in an IT disaster recovery plan? Is there a response team available to rapidly respond to incidents? Is there an escalation process for incident response to keep staff, management and stakeholders informed when an incident gets progressively worse or takes a long time to fix?
- Does the organisation have a priority list for restoration of IT services following an incident? Is there regular testing to provide assurance recovery can be achieved within acceptable timeframes?

Monitoring and reporting

- Are cyber security attempts and breaches formally reported and investigated? Is there independent review? Are these reported to senior management and the Audit Committee and Board in a timely way?
- Are sanctions imposed on employees and contractors who access information inappropriately or illegally outside their authorised access privilege limitations? Is there a defined process to deal with IT security violations?
- Are regular reviews and audits of information and cyber security arrangements performed and reported to senior management and the Audit Committee? Does this include regular penetration testing?
- Has the organisation's compliance with standards and good practice information and cyber security principles been formally assessed or audited? Have results been reported to senior management and the Audit Committee?

Some of the metrics that can be used by the Audit Committee to assess effectiveness of cyber security management:

- Detected intrusion attempts
- Incident rates
- Severity level of incidents
- Response times
- Time to remediation
- Costs of data breaches
- Costs of remediating cyber incidents

KPMG

© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

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: info@miod.mu **W:** miod.mu
Business registration number: C08077130

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained in Position Papers disseminated by the Audit Committee Forum is of a general nature, and is not intended to address the circumstances of any particular individual or entity. The views and opinions of the Forum do not necessarily represent the views and opinions of KPMG, the Mauritius Institute of Directors and/or individual members. These guidelines are for discussion purposes only and in considering the issues the culture of each entity should be taken into account as must the charter for each entity's Audit Committee. Although every endeavour is made 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 reliance should be placed on these guidelines, nor should any action be taken without first obtaining appropriate professional advice. The Audit Committee Forum shall not be liable for any loss or damage, whether direct, indirect, consequential or otherwise which may be suffered, arising from any cause in connection with anything done or not done pursuant to the information presented herein.

This publication does not provide guidance on how to deal with individual situations, nor does it provide a complete description of relevant legislation. Reference may need to be made to the legislation and other pronouncements mentioned in the text and to the organisation's professional advisers for detailed information.

© 2022 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.