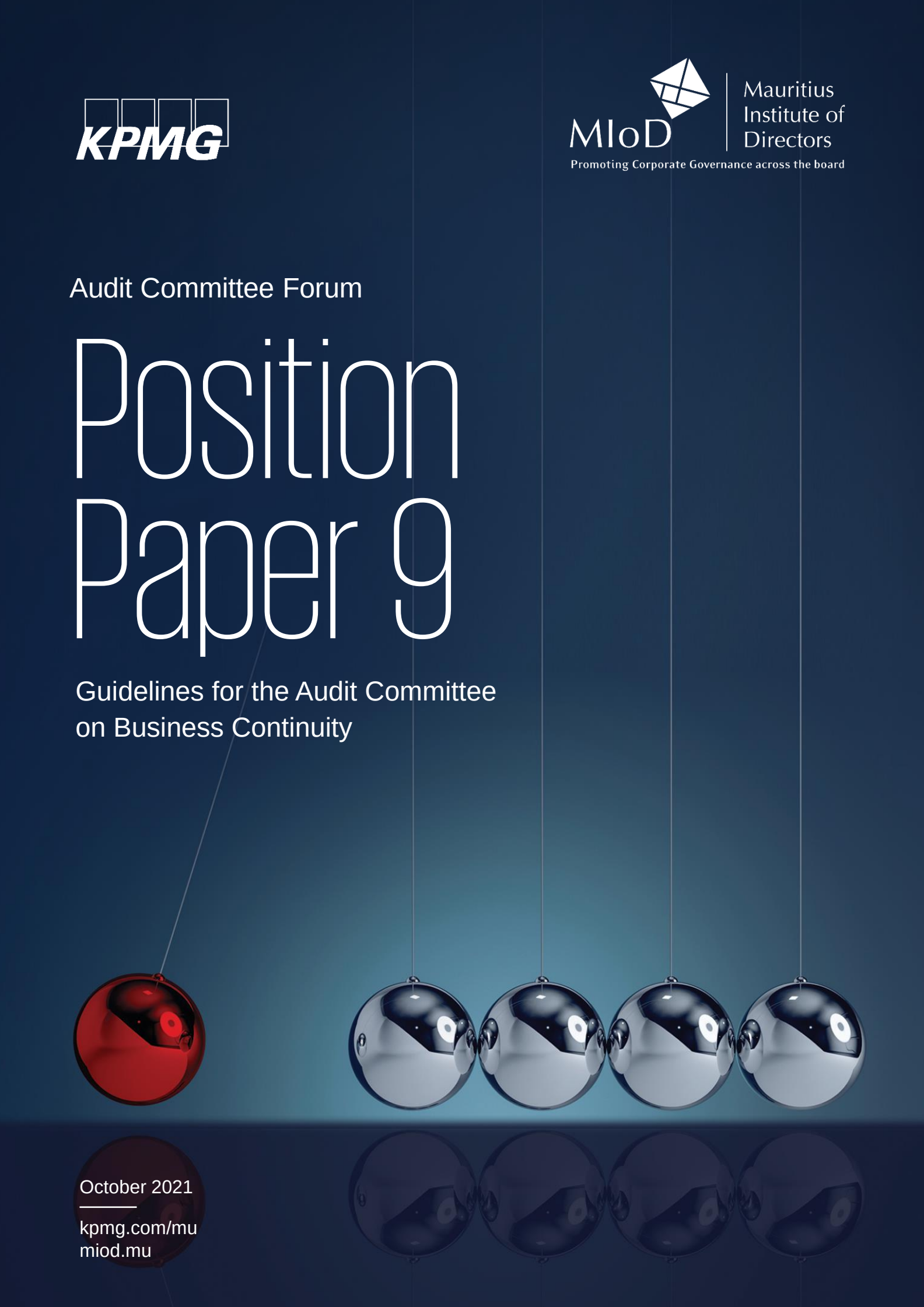
KPMG

MIoD
Mauritius Institute of Directors
Promoting Corporate Governance across the board

Audit Committee Forum

Position Paper 9

Guidelines for the Audit Committee on Business Continuity



October 2021

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 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 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 9 deals with Business Continuity.

Previous Position Papers are listed below and may be accessed at https://home.kpmg.com/mu/ and http://www.miod.mu/.

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's Guidelines for the Evaluation of Retirement Obligations (July 2019)

Paper 8: Audit Committee's guidelines on Data Protection (October 2020)

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
Chundoo Fouad
Chung John
Cundasawmy Robin
Dinan Pierre
Gooroochurn Bharatee
Ibrahim Nesmah
Kee Mew Mervyn
King Antoine

Secretary:
Bishundat *Varsha*

Kistnamah Nagesh
Koenig Fabrice
Leung Shing Georges
Leung Steve
Maigrot Sylvia
Molaye Sanjay
Mooroogen Sumita
Ong Su Lin
Ramdhonee Kalindee
Ramdin-Clark Madhavi

MIoD Co-ordinator:
Mulung *Nafeeza*

Contents

Sources that have been used in writing this Paper:

- *ISO. 2019. ISO 22301:2019: Security and resilience — Business continuity management systems. https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en*
- *World Economic Forum. 2021. The Global Risks Report 2021. 16th ed. http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf*

Introduction

Business continuity is a discipline that considers an organisation's ability to maintain essential functions during and after a disaster has occurred. Fire, flood, cyber-attack, disease outbreak, equipment breakdown, supply chain failure or losing a key employee are examples of disruptions that can happen to an organisation at any moment. The most basic business continuity requirement is to keep essential functions up and running during a disaster and to recover with as little downtime as possible. A Business Continuity Plan considers various unpredictable events, such as natural disasters, and other external threats. It is a framework which allows key functions of an organisation to continue even if the worst happens after unpredictable events and as such, acts as a medium to mitigate disruptions.

Historically, many organisations have developed business continuity plans to address situations where their buildings, systems, equipment, and products or services are damaged, with the assumption that at least a few employees can return to their work sites after the incident. However, as the COVID-19 outbreak has showed, when access to both employees and work sites is limited for a long period of time, it can severely impact an organisation's ability to recover.

In today's uncertain environment, the nature and importance of risks have evolved and it is evident that major disruptions can occur. In some instances, the disruptions could severely jeopardise the going concern viability of an organisation, leading to its management having to re-think the entire business strategy. As organisations navigate the ongoing COVID-19 crisis, there are a number of key issues that corporate leaders should be thinking about, as well as steps they can take to react to severe interruptions and also reshape their organisation, and plan for recovery.

Business Continuity Planning (BCP) establishes Risk Management processes and procedures that aim to prevent interruptions to mission-critical services, and re-establish full function to an organisation as quickly and smoothly as possible. The impact of risks varies by entity depending on the particular industry they operate in, and as such the business continuity plan needs to be entity-specific. Whilst technology was already vital to an organisation, the pandemic has further strengthened that position. Communication, work and education are almost impossible without technology today.

As organisations adjust their operations in the new normal, Boards of Directors must be aware that there are other risks, just as serious and as far-reaching, that sit right around the corner. Notably, The Global Risks Report identified environmental risks, namely climate change as part of the five most likely global threats for the coming decade (World Economic Forum 2021).

BCP remains the Board of Directors' responsibility, but the Audit Committee can play a pivotal role in ensuring that the Board remains committed to having an effective and sustainable business continuity plan.

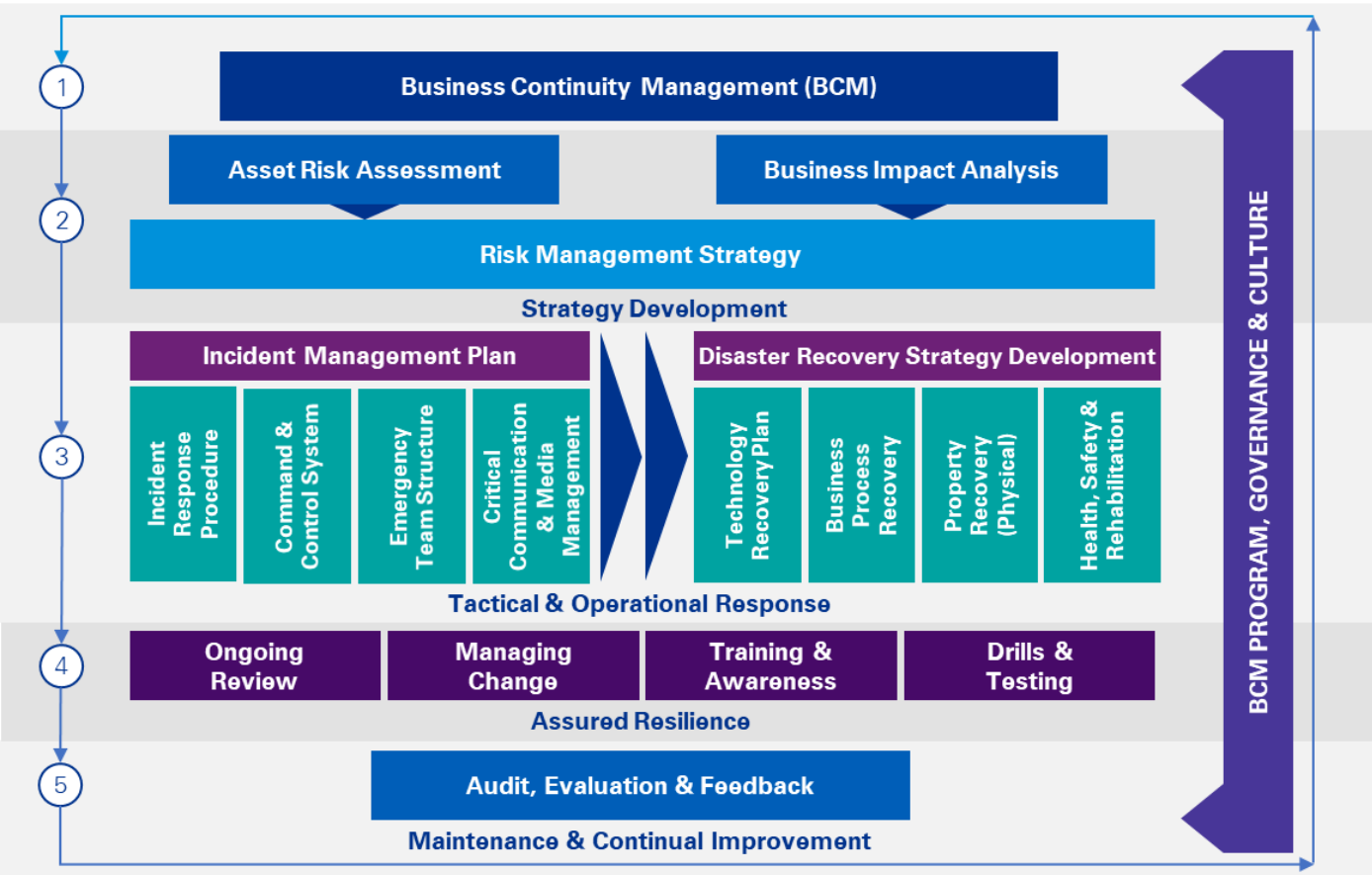
Evolution of Business Continuity

Business Continuity became a more formalised discipline in the 1980s, with a clearly defined mission to protect an organisation. Business Resilience began appearing in the Business Continuity vocabulary in the early 2000s and, at times, has been used interchangeably with Business Continuity, but the terms have different shades of meaning.

Business Continuity involves resuming operations from an incident once it has occurred and is process centric. In contrast, Business Resilience focuses on building an organisation to be impervious to potential disruptions of various kinds and is more strategic in nature. It is about preparedness for organisations to continue operations in the face of unexpected disasters by enhancing their immune system and also adapt and prosper post the disaster. ISO 22316:2017 defines organisational resilience as: "*The ability of an organisation to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper.*"

Business Continuity Management, Technology Disaster Recovery, Incident Response and Crisis Management are among the disciplines that shape an organisation's resiliency. The diagram below gives an insight into the interconnectedness of these disciplines, forming part of a typical Business Resilience Framework, which are developed further in this Paper.

Refer to Appendix 1 for definition of key terms.



Source: ISO 22301 – Business Continuity Management Framework (ISO 2019)

Management should be fully conscious that survival of their organisation depends on its resilience and that building and enhancing resilience is one of their primary responsibilities.

Furthermore, the Board of Directors / Audit Committee must address business resilience as part of their overall governance and risk management responsibilities to enable the organisation to survive and thrive in an increasingly hostile environment.

The Board of Directors must ensure that the Business Resilience framework is adapted to the nature, type and size of the business and ensures that shareholders' value is protected at times of disruption through a Value Protection Plan. Further, with the evolution of Business Resilience, certain mature organisations are also putting in place an exploitation plan which enables the organisation to spot and exploit commercial opportunities that may present themselves during times of substantial disruption.

Key principles that a Board of Directors must take into consideration when defining their Business Resilience strategy and framework:

i. Commitment and support from members of the Board of Directors and senior executives for enhancing organisational resilience

ii. Resilience framework to be situated in the context of the overall organisational Governance and Risk Management

iii. A common vision and purpose with behaviour aligning to same principles

iv. Diverse skills, leadership, knowledge, and experience to be on board

v. Identification of critical operations/areas for which resilience should be built in and identify interdependencies and vulnerabilities

vi. Indicators for critical operations which act as warning signs to activate responses

vii. Adequacy of resources and cost benefit analysis

viii. Systems to support implementation of the framework and resilience activities

ix. Effective communications with both internal and external stakeholders

x. Training and embedding a resilience culture across the organisation and stakeholders

xi. Rigorous testing of the framework in varied scenarios

xii. Evaluation and enhancement of the framework

Risk Assessment

Risk is present in all decisions and activities undertaken by organisations and a number of these will present continuity issues. The approach to managing continuity risks therefore, is to implement a Business Continuity Management (BCM) process.

Managing risks include avoiding, transferring and accepting the risks. BCM is one of the ways of mitigating risks to lessen the impact when they occur.

BCM, considered as a method of Risk Assessment, is defined by the Business Continuity Institute, as the act of anticipating incidents which will affect mission critical functions and processes for an organisation and ensuring its responsiveness to any incident in a planned and rehearsed manner whilst the business recovers.

Risk Identification

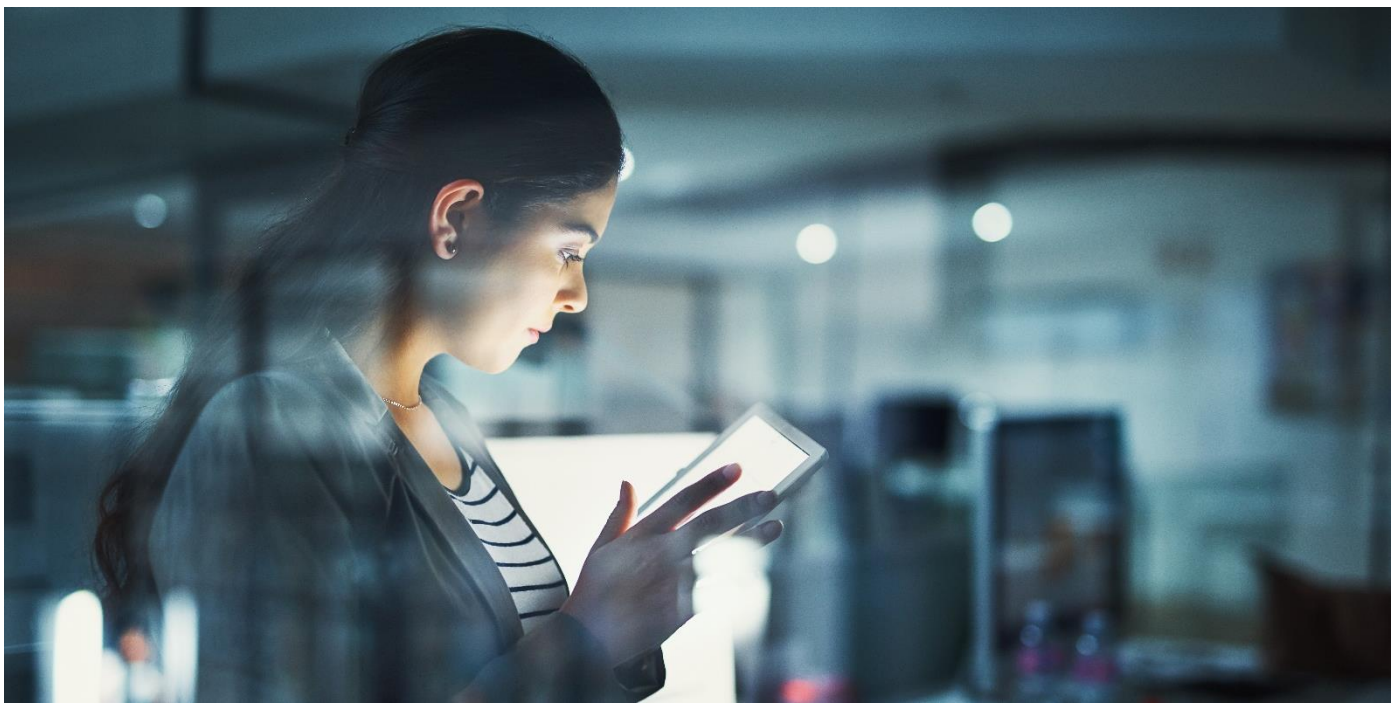
A critical aspect of Risk Assessment is the Risk Identification stage which involves thinking through the sources of risks, what can happen, the possible causes and consequences of the internal and external environment that can create uncertainties in the achievement of the organisation's objectives.

An organisation should focus on the effective management of the following potential sources of risks:

— Strategy;
— Operations;
— Safety;
— Financials;
— Human resources;
— Legal and regulatory (including the change in Government Policies);
— Governance;
— Industry;
— Technology (including information security);
— Reputation;
— Projects;
— Health & Safety; and
— Environmental.

Business Continuity Management (BCM) framework

Once the risks sources have been identified in an organisation, a BCM Framework is required to mitigate the risks and it is critical to establish ownership for successful implementation.



Key questions when identifying the risks are:

i. Who is responsible (risk owner)?

ii. What are the major business process objectives?

iii. What might undermine (i.e. prevent, degrade, or delay) the achievement of the objectives?

iv. What might accelerate or enhance the achievement of the objectives?

v. What is the likelihood of an event happening?

vi. When can they happen? (determine the time/s they can occur)

vii. Where can they happen? (determine the location/s)

viii. Why and how can they happen? (determine the causes of why and how it may or may not occur)

ix. What could the impact (consequence) be?

The purpose of the BCM Framework is to identify in advance the actions necessary and resources required to manage an interruption regardless of its cause.

This should be a formal documentation of an organisation's business continuity strategy and should be considered a live document i.e. which is regularly updated.

In terms of resources, the COVID-19 pandemic and other unforeseen circumstances have provided experience of how resources/materials are vital in a period of crisis.

Some basic elements, which are not exhaustive, that should be included in a BCM framework are:

— BCM leadership roles and responsibilities
— Business continuity plan approval
— Internal and external contact information including emergency services
— Utilities and facilities services
— Critical records and systems
— Back up locations and processes
— Back up service provider and supplier information
— Communication strategy to internal and external stakeholders

The written BCM framework should include a step-by-step procedure manual that is easily accessible to all stakeholders in an emergency situation.

Business Impact Analysis (BIA)

To successfully implement a BCM Framework, an organisation will need to undertake a thorough BIA to identify the critical activities that are essential for the smooth continuity of its business. Once the critical activities have been recognised therein, the BCM Framework can be used to reduce major disruptions and mitigate any major impact.

Senior Management needs to understand the organisation and the urgency with which activities and processes will need to be resumed in the event of a disruption. This includes performing an annual BIA which identifies, quantifies and qualifies the business impacts of a disruption to determine at what point in time the disruption exceeds the maximum acceptable recovery time. The determination is usually done separately for each key function of the organisation, while the risk assessment reviews the probability and impact of various threats to the organisation's operations.

This involves stress testing the organisation's business processes and the BIA assumptions with various threat scenarios.

General non-exhaustive risks that affect Business Continuity:

i. Unplanned IT and telecom outages

ii. Cyber attacks

iii. Data breaches

iv. Climate change

v. Interruptions to utility supply

vi. Fire

vii. Security incidents

viii. Health & Safety

ix. Associated risks related to COVID-19 pandemic

x. Acts of terrorism

xi. New laws or regulations

xii. Policy on movement and loss of key personnel

xiii. Reliance on third parties (contractors and subcontractors)

xiv. Force majeure

Business Continuity Management (BCM) Strategies

The results from a Risk Assessment should assist in refining the impact analysis to develop BCM strategies. Moreover, an organisation needs to determine and select which BCM strategies to use to continue its business activities and processes in the event of an interruption.

This includes determining how to manage the risks identified in the risk analysis process. The strategies should be determined at both the organisational and key functional levels.

BCM strategies for continuity and recovery are:

Diversification – of activities and resources to ensure continued operations at two or more geographically dispersed places.

Replication – by copying resources to enable operations to recover quickly in the replicated site is dormant and brought into live operation after an incident.

Standby – where a facility has been temporarily shut down but is capable of becoming operational at short notice.

Post-incident acquisition – documenting a list of recovery requirements detailing resources to be acquired after an incident occurs, upon having pre-qualified suppliers providing resources at short notice.

Subcontracting – whereby third parties can be used to produce products or services, provide infrastructure and undertake activities.

Insurance – by providing financial compensation for loss of assets, loss of revenue, increased costs of working, business resumption and protection of associated legal liabilities.

Accepting the risk – accept the risk following assessment of costs and consequences.

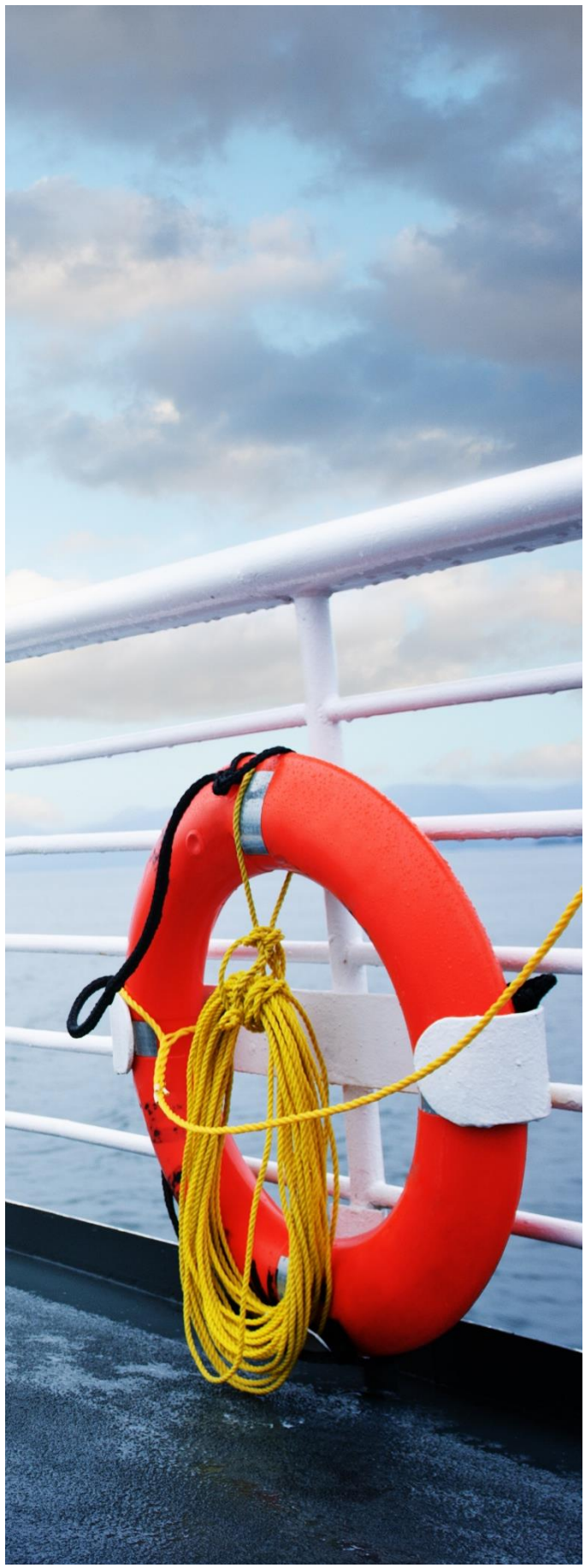
Updates to the Business Continuity Management (BCM) Framework

The BCM Framework should be reviewed, tested and maintained regularly.

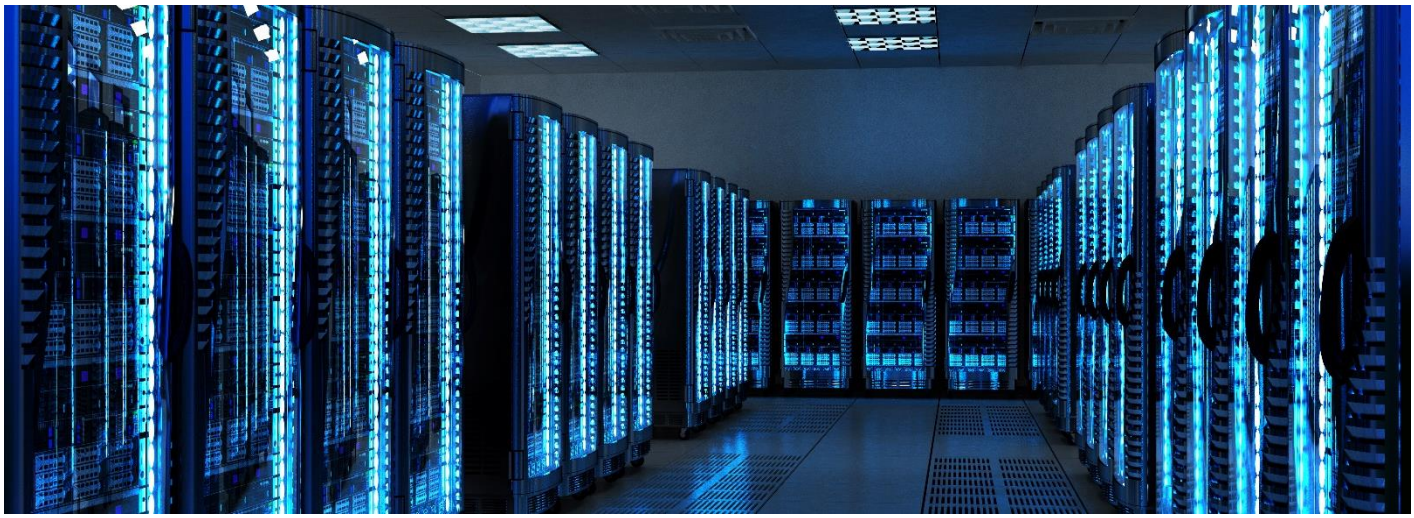
The testing should be based on a methodology that determines what should be tested, how often tests should be performed, how tests should be run, and how tests will be scored and documented.

It is recommended that key aspects of the plan be tested annually and that the tests be based on clear objectives that will allow the results of the tests to be scored to determine its effectiveness.

Regular testing should allow the organisation to identify any potential weaknesses due to internal and external changes.



Technology



Technology has surely evolved more rapidly over the past 20 years than during centuries ago.

Nowadays, technology is an integral part of our everyday life and many organisations rely heavily on technology to support their key business operations and strategies. Given that technology forms part of the core activities of most organisations, they are likely to lose money and/or reputation if they are unable to adequately operate due to unexpected technology failure and/or prolonged downtime.

For example, cyber risks are considered to be among the top risks faced by any business having access to the Internet, and such risks when materialised, can easily disrupt an organisation.

According to cyber security experts, it is not a question of what is the form of a cyber attack but when will it occur, and whether the organisation is prepared or not. However, an organisation which has put into place means to protect itself from cyber risks and/or defend itself against cyber attacks, is more likely to suffer less damages and be able to resume its business operations rapidly in the event of a cyber attack.

Therefore, disruptions arising from cyber attacks need to be on the top list of priorities of an organisation's agenda. To ensure that organisations using technology are able to recover promptly from IT failures and/or cyber attacks within an expected timeframe, it is essential that they have a Disaster Recovery Plan (DPR) ready to be deployed.

Disaster Recovery Plan (DRP)

A DRP is an approved document which details IT related policies, tools and procedures to execute in the event of an IT related incident/crisis. It is a subset of the various plans including in a BCP and needs to be aligned with the latter's objectives. Upon activation of the DRP, IT related recovery processes will be carried out to recover and/or protect the IT infrastructure and/or IT systems of the organisation both during and after a disaster (refer to Appendix 2 for potential contents of a DRP and a non-exhaustive list of IT systems).

When devising a DRP, an organisation needs to determine its Recovery Point Objective (RPO) or Recovery Time Objective (RTO). The RPO is the maximum amount of data loss acceptable by an organisation after a disaster while the RTO is the maximum amount of time acceptable by an organisation to resume its key operations after a disaster.

An organisation may face severe consequences, including insolvency, in case the amount of data loss (related to RPO) and/or amount of time (related to RTO) exceed the acceptable maximum limits.

Testing of a DRP is as critical as the formally documented DRP and requires the involvement of all relevant employees including service providers / key stakeholders especially if an organisation is highly dependent on its hardware, software or other IT related services for business operations.

Some organisations have a disaster recovery site in which they have backup/redundant IT infrastructure and systems that enable them to continue their business operations quickly following a disaster at their main office. It is also important that an organisation votes a budget for testing of the DRP and performs testing on a regular basis taking into consideration any significant changes made to the IT and or business environment.

It is also recommended to request Internal Auditors/IT Auditors to review the DRP on a regular basis especially when the organisation has undergone major changes regarding its IT systems.

Critical IT systems and service providers

It is essential to maintain an updated list of all IT systems used in an organisation including the latest updates as well as contact details of the corresponding suppliers. This is often the most challenging task of an IT department.

Also, having spare IT equipment and/or redundant IT systems may be costly for an organisation. Therefore, as part of a DRP, it is essential to identify critical IT systems and to ensure that they can be repaired, replaced, reconfigured within time limits set by an organisation.

Some organisations can afford to have a full-fledged IT department but this may not be the case for other organisations that prefer to outsource their non-core services including IT, while focusing on their key operations. Therefore, response time of service providers is critical especially following a disaster to ensure continuity of IT systems supporting business operations.

It is important for the organisation to maintain a list of critical IT systems together with contact details of respective service providers. Contact details may also include alternative suppliers providing the same IT equipment/resources being used by the organisation, as backup options.

It is important to have updated Service Level Agreements (SLAs) with service providers which includes their involvement and response time in the event of an incident or disaster. In case that the organisation outsources its IT systems or services to a service provider, the latter needs to have a formally documented and tested DRP to ensure minimal business disruption.

Depending on the needs and requirements of the organisation, it has to ensure that in the event of a disaster, it has sufficient resources (e.g. financial, manpower and business partners) to restore its IT services so that the business can continue to provide key products and/or services to clients with minimum disruptions.

Work From Home (WFH)

The COVID-19 pandemic has certainly accelerated the WFH scenario in Mauritius and other countries, whereby employees do not need to be at the office to perform their daily work and just need to use technology with connectivity to access company resources and/or use collaborative cloud platforms to work.

The probability of an employee being vulnerable to a cyber attack while working at home may be higher due to the home Wi-Fi network not as adequately secured as the office network.

Therefore, WFH may entail additional risks that an organisation has to take into consideration when allowing using technology at home including remote access to company's data and resources.

Additionally, an organisation has to identify critical IT systems used by employees working from home, as these IT systems need to be an integral part of the DRP. Security and backup of data may be a priority for those working from home especially if they are working on documents found on their laptops/mobile devices only.

Audit Committee's role on Business Continuity

Many organisations have contingency plans that were developed with an eye on disruptions to the micro-environment, such as power outages, inability of staffs to reach their workplace, and the unavailability of machinery.

However, such plans might not be adequate for the type of macro-environmental disruption we are currently experiencing which affects many, if not all, stakeholders in an organisation's ecosystem.

For now, organisations need to be managed in a highly challenging environment, that for some, is tantamount to a crisis. To succeed, strong leadership, and the need to adapt and improvise are required.

Organisations need to answer the following important questions:

— Are we fully prepared to face a crisis?
— Do we understand all potential risks?
— Have we thought "outside the box" regarding risks and responses?
— Are all responses documented?
— Do we have the right resources readily available to assist?

An effective response by an organisation requires transparency, accountability, and above all, strong leadership. Organisations need to be clear about who is making the decisions, keeping the Board of Directors regularly informed, and maintaining the Board's independence.

While the prime responsibility for ensuring that organisations have proper business continuity planning rests with the Board of Directors and senior management, Audit Committees need to understand their own responsibilities in this area.

The Audit Committee or Risk Management Committee, or if the Audit Committee is handling a combined role, can play a pivotal role in assessing management's approach to business continuity.

Increasingly, Audit Committees are expected to oversee risk management processes in order to ensure that financial reports clearly reflect an organisation's risks and exposures. An Audit Committee is required to understand how the risk management process is tailored to an organisation's specific needs, investigate whether the process is ongoing, ensure that the responsible individuals

have appropriate stature, expertise and time, and meet periodically with the Risk Officer.

As a result, whether specifically referred to or not in the Audit Committee charter, business continuity management is an integral part of the risk management framework within an organisation. As such, it should be included in the Audit Committee's oversight responsibilities.

The Audit Committees may find it difficult to assess whether the BCM process is adequate. Aspects that may provide some comfort include:

— Formal standardised policy and procedures, including IT disaster recovery plans; emergency response procedures; off-site storage of records; backup and recovery procedures; evacuation plans; communications strategies and media liaison strategies. Documented plans for different scenarios.

— Identified recovery locations. Testing of plans including the maintenance of adequate documentation of testing results.

— Training materials and evidence that regular training (awareness and specific) has been conducted. Adequate budget allocation for business continuity management.

— Service level agreements with service providers for the provision of services in the event of a disaster.

— Evidence that regulatory requirements are taken into account in the policy and procedures for disaster recovery; that requirements for daily Business Continuity are included in the Operational, Health, Safety, Security and Environmental policy, procedures and processes, and that compliance is monitored.

The Audit Committee can also obtain comfort regarding the adequacy of BCM by:

— Continuous discussions with executive and operational management on how the business continuity management process is managed in the organisation.

— Discussions with the Risk Officer to establish how BCM is integrated with the organisation's risk management processes, and whether adequacy assessments have been made.

— Reviewing the findings reports as shared by the Risk Officer.

— Engaging industry specific BCM experts to perform independent evaluation and benchmarking exercises.

— Utilising internal audit to perform audits, including benchmarking, of the BCM process (provided internal audit has the necessary skills to do so).

— If appropriate, peer reviews could also provide valuable benchmarking information.

Developing increased resilience to strategic risks or improving 'Risk Resilience' requires risk management, disaster recovery and other disciplines to work together.

The Board of Directors and the Audit Committee have two main roles in relation to BCM:

Under normal business conditions

To ensure that the organisation, including the Executive Team and Board members are ready to deal with a crisis; an Audit Committee should be seeking this assurance through its oversight of internal audit and related activities on behalf of the Board of Directors.

An Audit Committee should ensure that the organisation has a robust crisis communications strategy that engages customers, employees and other stakeholders as part of the organisation's crisis planning and preparations.

Some key questions that an Audit Committee should ask are:

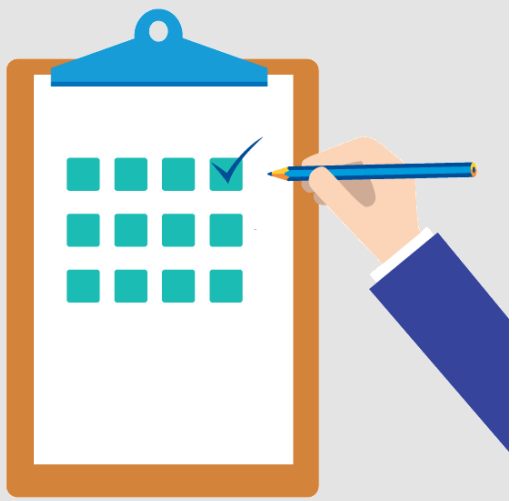
— Do we have a BCM plan, with clear roles and responsibilities, and who in the Executive Management Team (EMT) is responsible for it?
— Has our EMT been adequately trained and have they taken part in crisis simulation rehearsals; when was the last time they did so?
— Is there a Crisis Plan for the Board of Directors and have key Board members taken part in crisis simulation rehearsals?
— Is there a robust crisis communications plan and has it been 'stress tested' through crisis simulation rehearsals, including the how and by whom?
— What is the organisation's perception of vulnerabilities and key risks and its confidence in the preparedness to deal with such events should they arise?
— Has our BCM capability been subject to internal audit or external validation?
— Does the Audit Committee have access to any third party evaluation reports conducted on the BCM capability of the organisation?
— Does the organisation have adequate insurance coverage?

During and immediately after crisis

To act in a crisis (often in support of the EMT, though at times this may include replacing or standing in for key Executives) and to ensure lessons are learnt after the crisis; Audit Committee members should ensure that independent investigations and reviews post-event are undertaken where appropriate.

Key questions that an Audit Committee should ask:

— Is it clear which members of the Board of Directors will be responsible for what during a crisis?
— Is the organisation communicating appropriately and transparently to all stakeholders?
— Do we know who we would call upon to support the Board of Directors and are arrangements for same already in place?
— As a matter of course, do we demand an independent review in the wake of a crisis such that lessons may be learned and improvements made in the spirit of full transparency?



Conclusion

Believing a business will continue to generate profit in the future without putting safeguards in place is a very risky practice. Ignoring the pitfalls can be catastrophic. Success during a crisis or economic downturn will be determined by the level of business resilience for which strong leadership is required with the ability to adapt and improvise as conditions change.

Organisations must ensure the safety of their employees, compliance with relevant laws, the protection of their brands and ensure continuity of operations. Business Continuity needs to be seen as a safety net for organisations. Even though there are costs involved, it is well worth having such plans as it will save an organisation during an incident and help it react in an ordered and timely matter. Good business continuity plans, which are implemented successfully during a crisis, will give an organisation good return of investments and hence Business Continuity Planning (BCP) can be seen as a business enabler.

The pandemic has shown us the dangers in not anticipating risks – and severe risks may be just around the corner. Amongst others, it is time now to add climate risk to the Board of Directors' agenda as this is a likely global threat for the coming decade. Some examples of climate risk include heat waves, flash floods, rising sea levels, amongst others. Climate change may differ from other risks an organisation faces due to the potential magnitude of its consequences, but the Board of Directors can still adopt risk management oversight best practices to cope with it.

Building resilience has become a core skill. Continuity plans have to move out of theory and permeate into the real world. Events have to be planned and rehearsed through wide-scale, real-world simulations, and refined. A Board of Directors should be properly geared before a crisis hits and should have plans in place to protect an organisation, its employees, and its position within the marketplace. Board debates, now more than ever, should be open and broad. Organisations which will survive are those that are the most resilient.

> "One cannot be prepared for something while secretly believing it will not happen."
>
> **Nelson Mandela**

Appendices

Appendix 1

Definitions

Business Continuity consists of a plan of action. It ensures that regular business will continue even during a disaster.

Business Continuity Planning (BCP) is a strategy that ensures continuity of operations with minimal service outage or downtime.

Business Continuity Management (BCM) is defined as the advanced planning and preparation of an organisation to maintaining business functions or quickly resuming after a disaster has occurred.

Business Impact Analysis (BIA) predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies. Potential loss scenarios should be identified during a risk assessment.

Crisis management is the application of strategies designed to help an organisation deal with a sudden and significant negative event. A crisis can occur as a result of an unpredictable event or an unforeseeable consequence of some event that had been considered as a potential risk.

Business resilience is the ability an organisation has to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets and overall brand equity.

Disaster recovery is a subset of business continuity planning.

Disaster Recovery Plan (DRP) involves restoring vital support systems. Those systems are mostly communications, hardware, and IT assets. Disaster recovery aims to minimize business downtime and focuses on getting technical operations back to normal in the shortest time possible.

An **Incident Response plan** is the guide for how an organisation will react in the event of a security breach. Incident response is a well-planned approach to addressing and managing reaction after a cyber attack or network security breach. The goal is to minimise damage, reduce disaster recovery time, and mitigate breach-related expenses.

Appendix 2

Disaster Recovery Plan

Potential contents of a DRP

The contents of a DRP may differ depending on the type of organisation and/or its reliance on technology/IT systems, but generally includes the following main sections:

— Objectives of the DRP
— Risk assessment focusing on technology
— List of critical IT systems and supplier contact details
— Recovery procedures of IT related systems and training of relevant key staff
— Testing plan of the DRP
— Review and updates of the DRP
— Communication plan upon activation of the DRP

Non-exhaustive list of IT systems

— Hardware (e.g. servers, computers, laptops, printers)
— Software (e.g. office tools, antivirus, mobile applications)
— Network and connectivity (e.g. cables, switches, Wi-Fi, mobile data, VPN)
— Telephony and mobile devices (e.g. IP phones, tablets, smartphones)
— Firewall and other IT security systems
— Databases
— Cloud computing

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