ORGANISED BY SIAS

SUPPORTED BY CHARITY COUNCIL

CHARITY GOVERNANCE CONFERENCE AND WORKSHOPS 2021

DIGITALISATION
FROM RISK MANAGEMENT TO RISK RISILENCE

Mr Irving Low
Co-Head of Advisory
KPMG

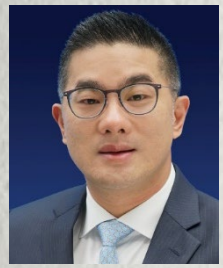
KPMG

Digitalisation: From Risk Management to Risk Resilience

Irving Low

29 September 2021

With you today



Irving Low
Co-Head of
Advisory
KPMG Singapore

Irving is a partner in KPMG in Singapore and has been with KPMG for over 28 years, having worked in both the London and Singapore offices. As the Co-Head of Advisory (Singapore and Indonesia), he is responsible for the Advisory businesses and practices across Management Consulting and Risk Consulting. Irving sits in the firm's Senior Executive Committee which oversees the firm's strategic and operational excellence. His key area of practice is in corporate governance, where he is also the KPMG APAC Leader for Board Advisory Services. He has undertaken numerous corporate governance reviews for both public and private organisations in light of the renewed focus in this area. He is a frequent invited guest and speaker at board meetings and presentations as well as public forums on corporate governance.

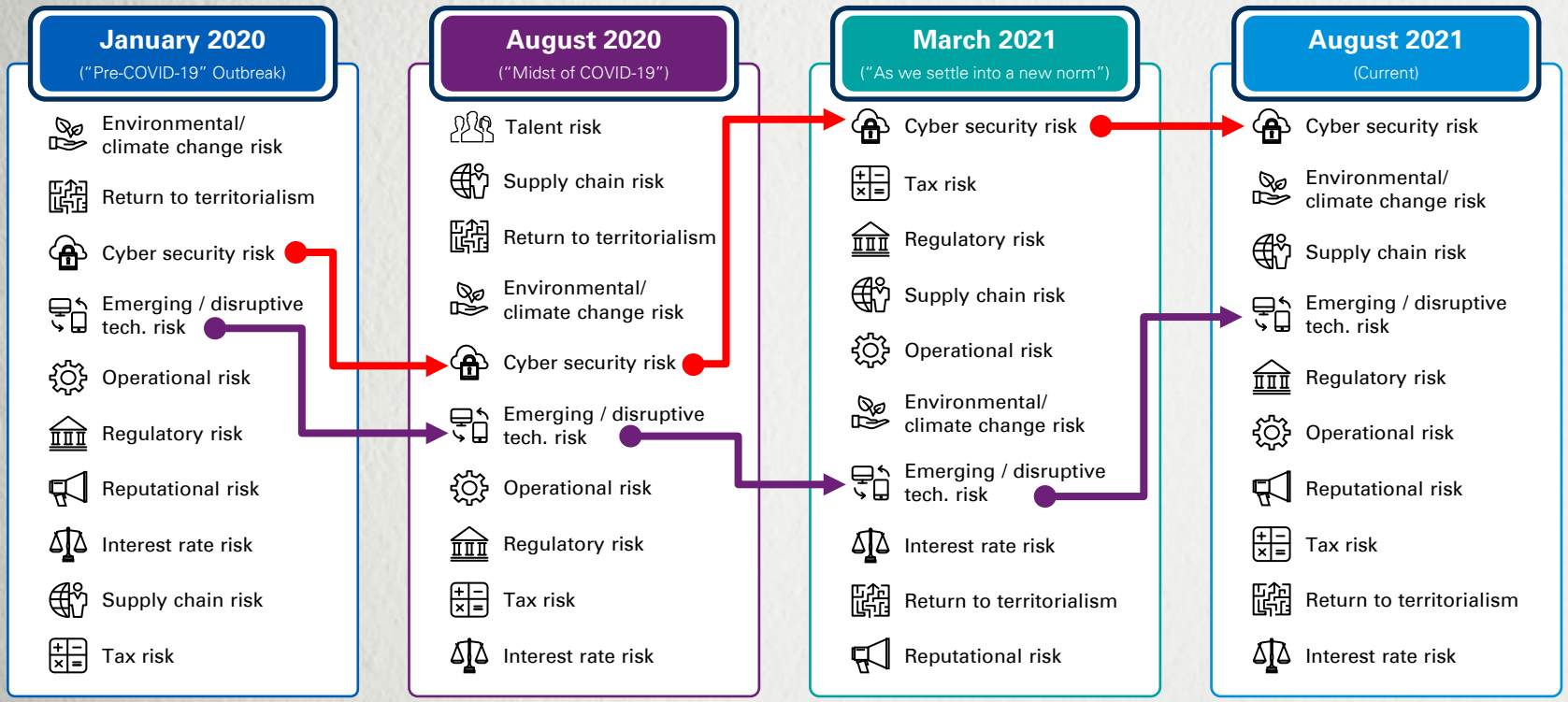
In October 2018, Irving was appointed to the Board of the Singapore Tyler Institute (STPI). He was also appointed on that same year to the Advisory Board for the School of Accountancy for the Singapore Management University. Together with the other Board of Advisors, they are tasked to help shape the future of the accounting profession.

In addition, Irving is a member of the Institute of Singapore Chartered Accountants (ISCA) where he is a member of the Governance Committee and the chairperson of CPA Australia Sub-committee for the Public Sector.

KPMG

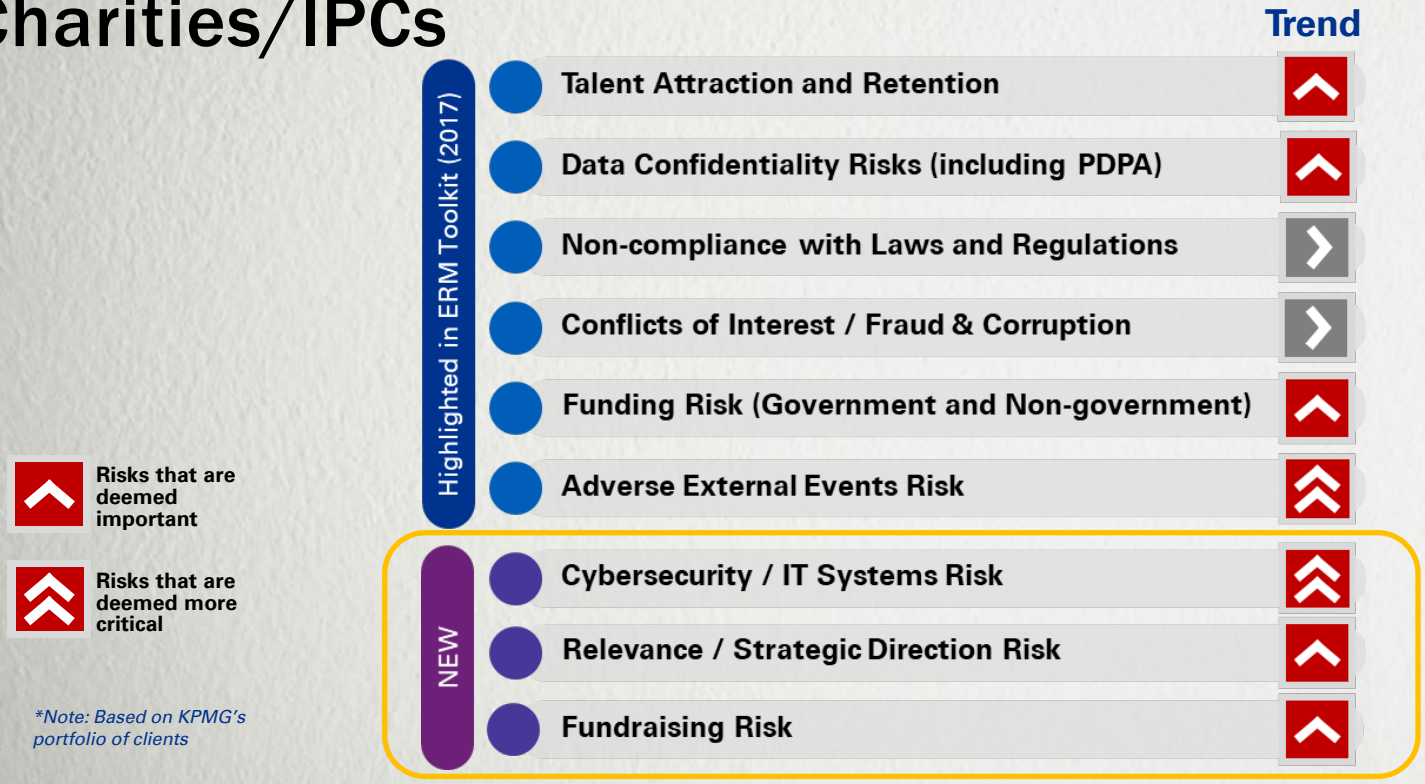
A changing risk landscape

Risk concerns change with more clarity



Source: KPMG CEO Outlooks; KPMG 2021 CEO Outlook draws on the perspectives of 1,325 CEOs across 11 major markets

Recent changes in top risks and concerns to Charities/IPCs



Note: Based on KPMG's portfolio of clients

ORGANISED BY SIAS
SUPPORTED BY CHARITY COUNCIL

Technology – Risk or Opportunity

Charities to receive help with IT services

…Charity organisations can look forward to greater aid in managing their IT systems with the new non-profit IT cloud service…collaboration between the Singapore Pools and NCSS…

Source: Straits Times

Crowd Funding an opportunity, not threat to Charities

…ability to reach out to a lot more donors and increase their exposure among the public… Code of Practice for Online Charitable Fundraising to boost transparency and accountability…

Source: Straits Times

Smart Nation initiative

…We envision a Smart Nation that is a leading economy powered by digital innovation… gives our citizens the best home possible and responds to their different and changing needs.…

Source: Smartnation.sg

Updated NRIC Rules to Enhance Consumer Protection

…From 1 September 2019, organisations are expected to stop collecting, using or disclosing customers' NRIC and other national identification numbers where it is not required under the law.…

Source: PDPC

Recent events in the news...

$40 million SkillsFuture Fraud case

…largest case of fraud perpetrated against a public institution in Singapore…

Singapore's HIV registry records leaked

…Confidential information of 14,200 people with HIV – including their names, contact details and medical information – had been stolen and leaked online…

SingHealth Cyber Attack

…1.5 million patients, including the outpatient prescriptions of Prime Minister Lee Hsien Loong and a few ministers, were stolen…

Personal information of 800,000 blood donors exposed

…personal information was exposed on the Internet for a period of nine weeks, after the data was mishandled by a vendor of HSA…

Non-Profits & Cyber Security – Facts & Figures

Charity Commission

Of charities in the UK think cybercrime is a major risk

Cyber Breaches Survey

Of non-profit breaches were a result of phishing attacks

Forrester Research

Increase in Covid-19 Phishing attacks in the first quarter of 2020.

Sources: Preventing Charity Cybercrime – Charity Commission For England and Whales 2019,
Cybersecurity Breaches Survey – Ipsos MORI 2021,
Forrester Blog - Forrester Research 2020

KPMG

Being Risk Resilient

ORGANISED BY SIAS | SUPPORTED BY CHARITY COUNCIL

Risk Management Requirements under the Code of Governance for Charities / IPCs

6.1.4 – Intermediate

The Board should ensure that there is a **process to identify, regularly monitor and review the charity's key risks.** This should cover mitigating measures and controls for all key risks

...Extracted from Code of Governance 2017

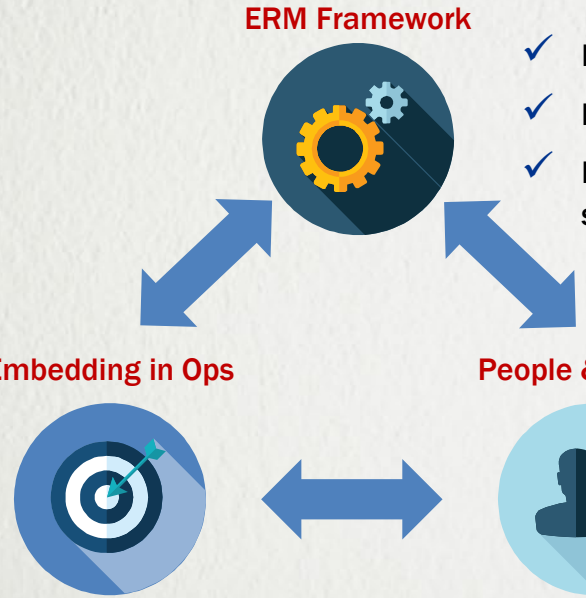
What the implications?

A The Charity is required to **forecast and evaluate** Financial, Compliance and Operational risks based on **likelihood** of risk occurrence and **impact** of risks.

B Requirements for the Board to understand and establish Risk Universe & Risk Parameters

Observations on risk management practices in Charities

- ✓ Linking of strategies and risk management; exploring the "relevance" of their activities with changing landscape
- ✓ Common 'gaps' uncovered by ERM include:
  - PDPA framework
  - Tech & Cybersecurity concerns
  - **Business Continuity Management (BCM)** and crisis management



- ✓ Increased adoption of ERM among Charities
- ✓ Documented ERM framework / policy
- ✓ Improving maturity of ERM among stakeholders

- ✓ Improved overall risk awareness
- ✓ Board risk oversight role – Majority adopting ARC
- ✓ Risk awareness at operational levels should be continuously built

Risk governance

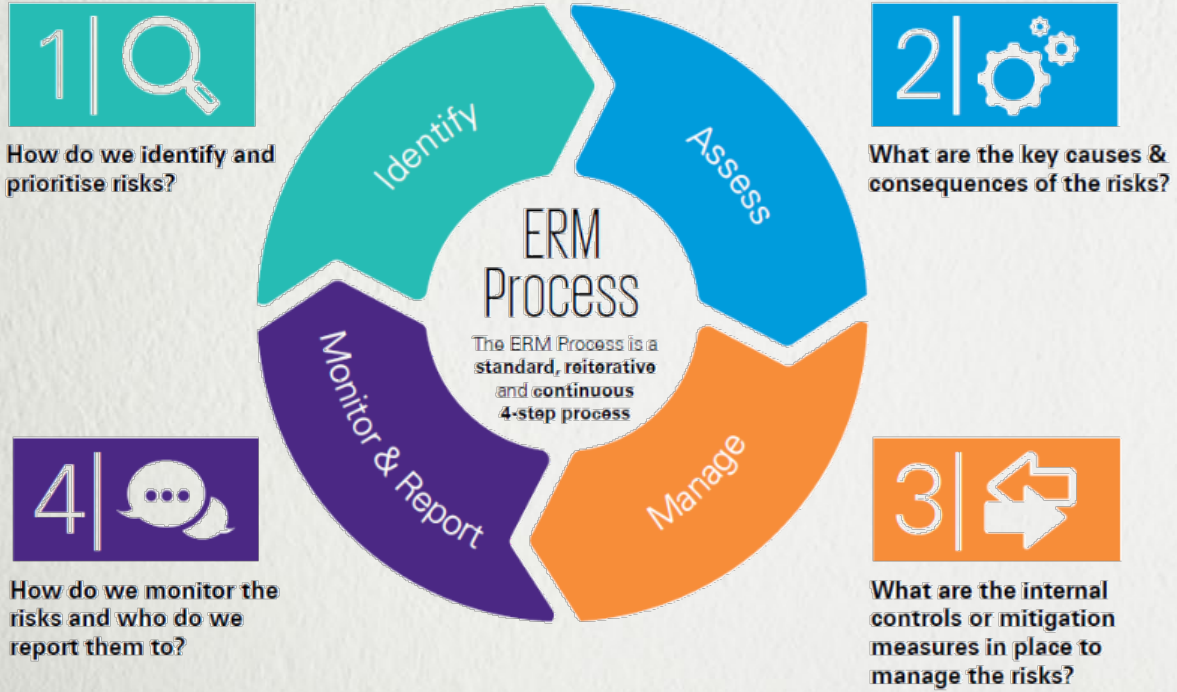
What is it?

Risk governance encompasses an organization's efforts to direct, manage, and report risk management activities across the enterprise based on the "Four Lines of Defence" principle.

KPMG 4 LINES OF DEFENCE

- Board sets the tone from the top and oversees the 1st, 2nd and 3rd lines of defence.
- Culture and conduct should permeate the entire organisation
- Foundation of the organisation is 'People, processes and systems"
- External assurance and regulators provide the final layer of protection to ensure that risks are managed adequately and effectively.

Starts with an enterprise-wide view of risks



ORGANISED BY SIAS | SUPPORTED BY CHARITY COUNCIL

Establishing a Tier 1 risk profile

Risk Universe

Strategic

S1	Education & Outreach
S2	Rising Public Expectations
S3	Corporate Branding
S4	Succession Planning Risk
S5	Relevance Risk
S6	Change in Government Policy

Financial

F1	Funding (Government & Non-Government)
F2	Fraud & Corruption
F3	Investment Risk
F4	Procurement Risk
F5	Donation (Fund) Utilization

Compliance

C1	Non-compliance with Laws and Regulations

Operational

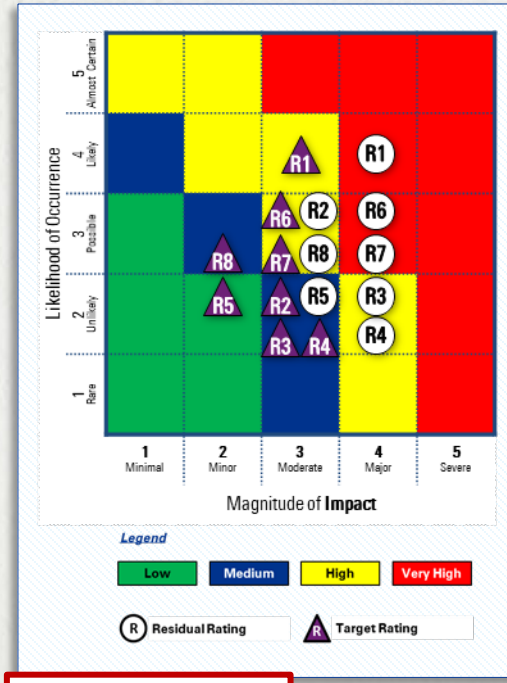
O1	Medical Service Incidents
O2	Pharmaceutical Management
O3	Workplace Health & Safety
O4	Adverse External Events Risk
O5	Media Publicity Risk
O6	Talent Attraction & Retention
O7	Outsourcing Risk
O8	Contract Management Risk
O9	Project Management Risk
O10	Volunteer Management
O11	Facilities Management
O12	Data Confidentiality

Technology

T1	Cybersecurity
T2	IT System Downtime
T3	Data Integrity Risk

ILLUSTRATION ONLY

Risk Prioritisation

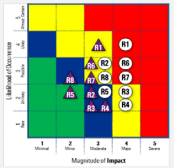


Ref.	Tier 1 Risk Profile
R1	Talent Attraction & Retention
R2	Data Confidentiality
R3	Non-compliance with Laws and Regulations
R4	Fraud & Corruption
R5	Funding Risk (Government & Non-Government)
R6	Adverse External Events Risk
R7	Cybersecurity
R8	Relevance Risk

ILLUSTRATION ONLY

ORGANISED BY SIAS
SUPPORTED BY CHARITY COUNCIL

Role of Internal Controls in Risk Management



Key risks to the organisation based on likelihood of occurrence and significance of impact

Controls are **processes, systems, or any other measures** put in place to **prevent, detect or respond** to the risk so as to reduce the likelihood or impact of the risk.

Adequacy (Design)

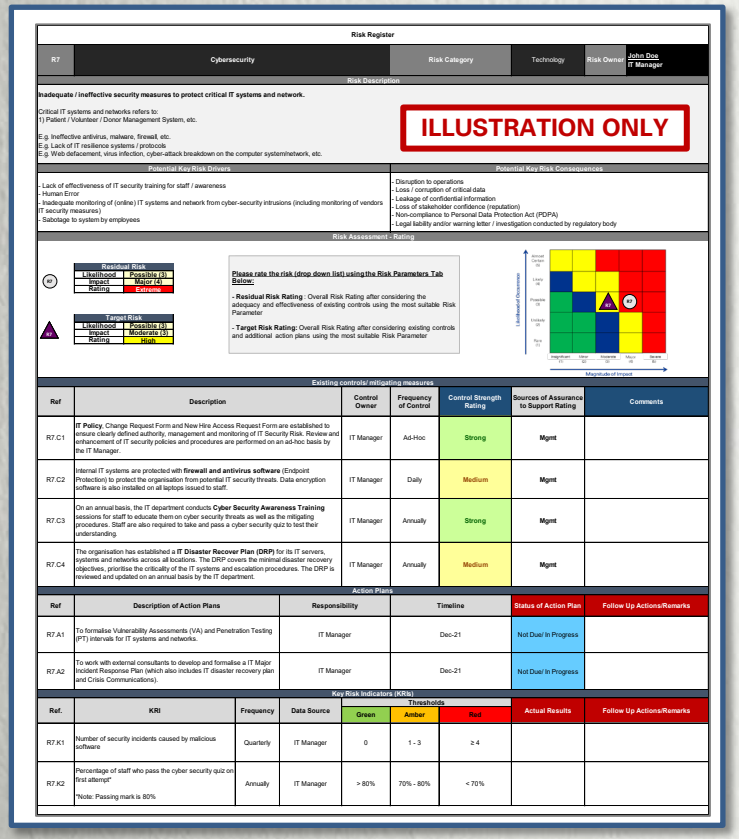
How the control is designed and whether it can mitigate the risk. A well-designed control can mitigate the risk identified.

Operating Effectiveness

Whether a well-designed control is consistently performed/ performed in the way it was designed for.

ORGANISED BY SIAS
SUPPORTED BY CHARITY COUNCIL

Managing risks using the risk register



Risk Register

R7	Cybersecurity	Risk Category	Technology	Risk Owner	John Doe, IT Manager

Risk Description

Inadequate / ineffective security measures to protect critical IT systems and network.

Critical IT systems and networks refers to:
1) Patient / Volunteer / Donor Management System, etc.

E.g. Ineffective antivirus, malware, firewall, etc.
E.g. Lack of IT resilience systems / protocols
E.g. Web defacement, virus infection, cyber-attack breakdown on the computer system/network, etc.

ILLUSTRATION ONLY

Potential Key Risk Drivers	Potential Key Risk Consequences
- Lack of effectiveness of IT security training for staff / awareness - Human Error - Inadequate monitoring of (online) IT systems and network from cyber-security intrusions (including monitoring of vendors IT security measures) - Sabotage to system by employees	- Disruption to operations - Loss / corruption of critical data - Leakage of confidential information - Loss of stakeholder confidence (reputation) - Non-compliance to Personal Data Protection Act (PDPA) - Legal liability and/or warning letter / investigation conducted by regulatory body

Risk Assessment / Rating

Residual Risk	
Likelihood	Possible (3)
Impact	Major (4)
Rating	Extreme

Target Risk	
Likelihood	Possible (3)
Impact	Moderate (3)
Rating	High

Please rate the risk (drop down list) using the Risk Parameters Tab Below:

- **Residual Risk Rating**: Overall Risk Rating after considering the adequacy and effectiveness of existing controls using the most suitable Risk Parameter

- **Target Risk Rating**: Overall Risk Rating after considering existing controls and additional action plans using the most suitable Risk Parameter

Existing controls/ mitigating measures

Ref	Description	Control Owner	Frequency of Control	Control Strength Rating	Sources of Assurance to Support Rating	Comments
R7.C1	**IT Policy**, Change Request Form and New Hire Access Request Form are established to ensure clearly defined authority, management and monitoring of IT Security Risk. Review and enhancement of IT security policies and procedures are performed on an ad-hoc basis by the IT Manager.	IT Manager	Ad-Hoc	Strong	Mgmt	
R7.C2	Internal IT systems are protected with **firewall and antivirus software** (Endpoint Protection) to protect the organisation from potential IT security threats. Data encryption software is also installed on all laptops issued to staff.	IT Manager	Daily	Medium	Mgmt	
R7.C3	On an annual basis, the IT department conducts **Cyber Security Awareness Training** sessions for staff to educate them on cyber security threats as well as the mitigating procedures. Staff are also required to take and pass a cyber security quiz to test their understanding.	IT Manager	Annually	Strong	Mgmt	
R7.C4	The organisation has established a **IT Disaster Recover Plan (DRP)** for its IT servers, systems and networks across all locations. The DRP covers the minimal disaster recovery objectives, prioritise the criticality of the IT systems and escalation procedures. The DRP is reviewed and updated on an annual basis by the IT department.	IT Manager	Annually	Medium	Mgmt	

Action Plans

Ref	Description of Action Plans	Responsibility	Timeline	Status of Action Plan	Follow Up Actions/Remarks
R7.A1	To formalise Vulnerability Assessments (VA) and Penetration Testing (PT) intervals for IT systems and networks.	IT Manager	Dec-21	Not Due/ In Progress	
R7.A2	To work with external consultants to develop and formalise a IT Major Incident Response Plan (which also includes IT disaster recovery plan and Crisis Communications).	IT Manager	Dec-21	Not Due/ In Progress	

Key Risk Indicators (KRIs)

Ref.	KRI	Frequency	Data Source	Thresholds: Green	Thresholds: Amber	Thresholds: Red	Actual Results	Follow Up Actions/Remarks
R7.K1	Number of security incidents caused by malicious software	Quarterly	IT Manager	0	1 - 3	≥ 4		
R7.K2	Percentage of staff who pass the cyber security quiz on first attempt* *Note: Passing mark is 80%	Annually	IT Manager	> 80%	70% - 80%	< 70%		

01 Main objective of the risk registers is to document **in-depth assessment** of the organisation's Tier 1 risks.

02 Risk registers should capture only the **KEY information** assessed for each Tier 1 risk.

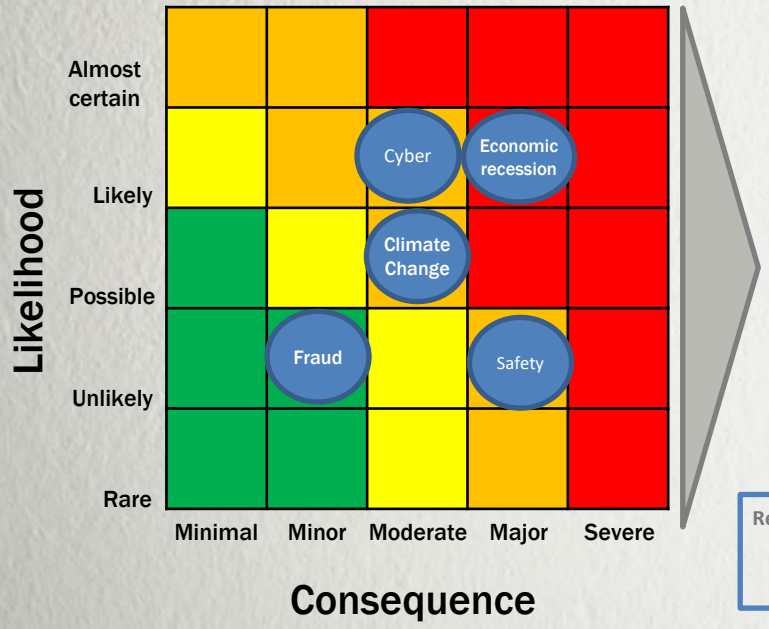
Documentation of the risk registers include:

- Risk Category
- Risk Description
- Risk Owner
- Risk Drivers & Consequences
- Risk Rating (Residual and Target Levels)
- Existing Controls / Mitigating Measures
- Action Plans
- Key Risk Indicators (KRIs)

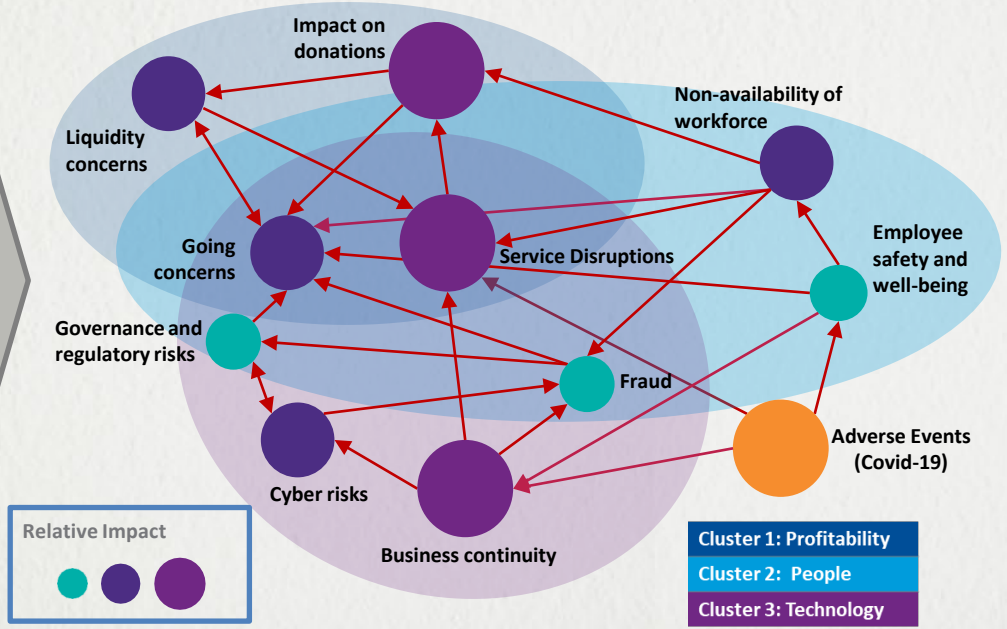
ORGANISED BY SIAS | SUPPORTED BY CHARITY COUNCIL

Making sense of risk in an interconnected world

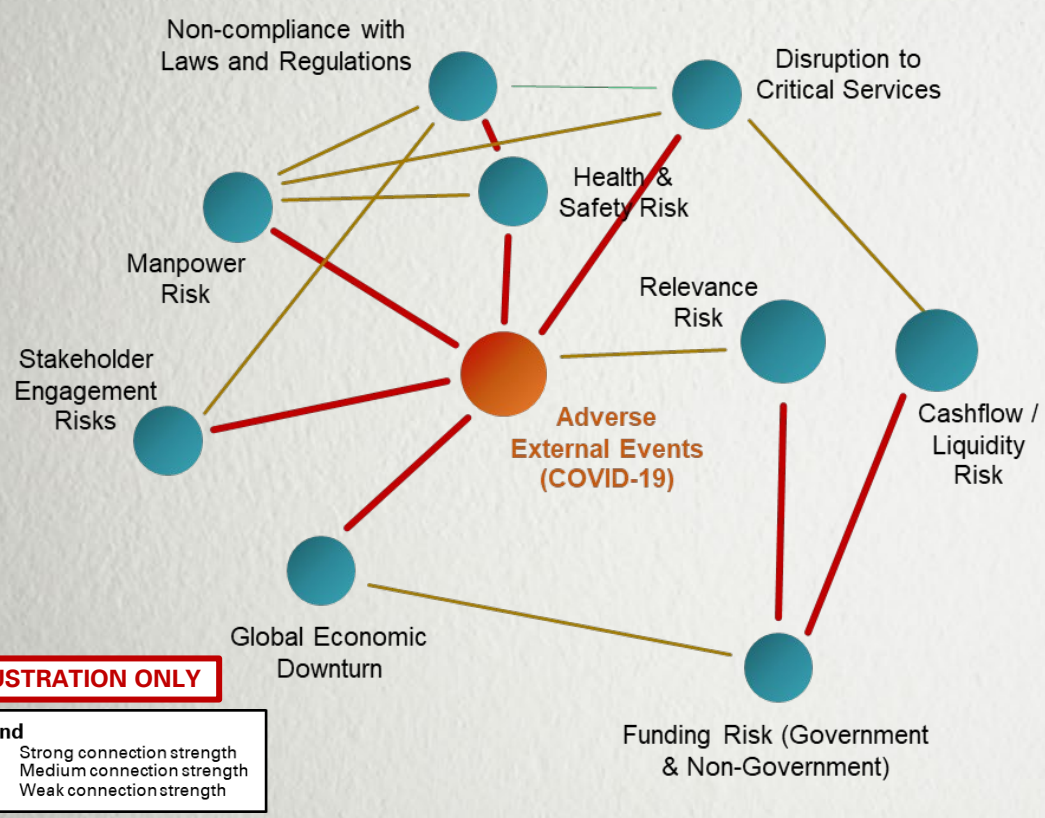
Traditional 'static' view



Dynamic 'connected' view



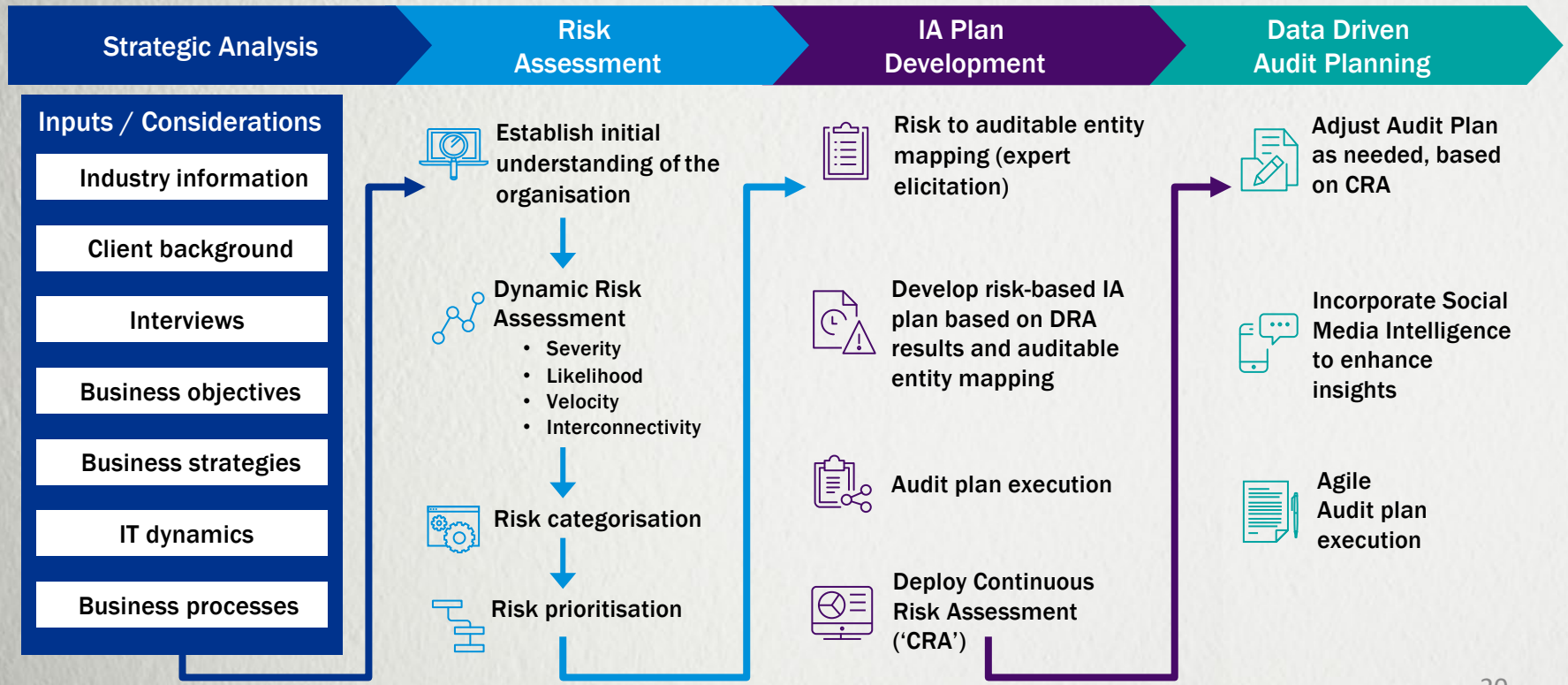
Integration of ERM and BCM



Some Key Considerations

- ✓ Is this a risk / threat to the organisation?
- ✓ How do we manage it?
- ✓ What Business Continuity considerations are there when managing Covid-19?
- ✓ What else should our BCPs cover to manage the network of risks and threats?

Risks and internal audit



What is Operational Resilience?

"Operational resilience is the ability of an organisation to **adapt rapidly** to changing environments. This includes both the **resilience of systems and processes** and more generally the ability of the organisation to **continue to operate its business** in the face of adverse operational events by anticipating, preventing, recovering from, and adapting to such events."

Operational Resilience in the New Reality

Resilience

Rapid response

Example:
- Crisis management teams and method/ tool support
- Urgent controls

Recovery

Risk management optimisation

Example:
- Catch up on the control "deficit"
- Obsolete controls
- Cost of control reduction and automation

New Reality

Risk management evolution

Example
- Enterprise resilience
- Security and privacy by design
- Digital trust (privacy, cyber, fraud and Customer experience)
- Automaton enablers

Redesigning the strategies and risk management target operating model

Cyber response during heightened COVID-19 threat

Strategic priorities amplified since COVID-19

- Driving revenue/donations
- Improving CX
- Creating a digital business model

- Adding new digital capabilities
- Building new digital products and services
- Building new digital platforms for customer-facing systems

Source: A commissioned study conducted by Forrester Consulting on behalf of KPMG, July 2020

Considerations for organisations

Have we identified and documented our key/critical/ important business services from the perspectives of our own organisation, our potential impacts on our stakeholders and, our potential impacts on the wider system?

Do we have effective engagement at Board level, and have we assigned clear responsibilities across the organisation?

Do we have a robust communication strategy for our key stakeholders?

Do we have appropriate resources to address capacity and capability risks? Is more and/or specialised resource required?

How does operational resilience support our growth agenda and engagement strategy? How can it drive improved performance?

Is there an ongoing, organisation-wide awareness and training program established around cybersecurity?

What key risk indicators should we be reviewing to manage risk at the executive management and board levels?

KPMG

Questions?

KPMG

Thank you

Contacts

Irving Low
Co-Head of Advisory
KPMG Singapore

T: +65 6213 2071
E: irvinglow@kpmg.com.sg