COVID-19 AND MANAGING BUSINESS RISKS

Jacob Elkhishin, Partner, RSM Australia
Roger Darvall-Stevens, Partner, RSM Australia

Speakers

Jacob Elkhishin, Partner, RSM Australia

Jacob is a Partner in the Risk Consulting division in Brisbane. Jacob has over 15 years' experience in the provision of internal audit, enterprise risk management, compliance audit, and environmental assurance services working with both public and private sectors. Jacob has assisted clients in the Energy Industry (Electricity, Oil and Gas), Transport, Infrastructure and the Public Sector. Jacob works closely with Senior Management and regularly presents reports to Boards and Audit Committees

Roger Darvall-Stevens, Partner, RSM Australia

Roger is the National Head of Fraud & Forensic Services at RSM Australia. He has over 30 years of experience in forensic accounting, forensic investigations of a range of matters (i.e. fraud, bribery, corruption, and workplace improper conduct such as bullying and harassment), fraud and corruption control (prevention including training, detection, response, and foreign bribery and corruption compliance advice), forensic technology (forensic IT and forensic data analytics), operation of whistleblower reporting avenues and management advice, and forensic due diligence. Prior to RSM, Roger was a Partner in forensics for a 'Big 4' firm (EY) where he was for 13 years, and initially commenced his career in the police force leaving as a detective after 12 years.

COVID-19: STRATEGIES FOR MITIGATING RISKS IN YOUR BCPS

Jacob Elkhishin, Partner, Risk Consulting Services, RSM

RSM

What we will cover

- Overview of disruption related risks
- COVID-19 Importance of Business Continuity Management
- Fundamentals of Business Continuity Management
- Recovery strategy implementation and monitoring
- Time-based scenario monitoring
- Questions and answers

Overview of Disruption Related Risk

Disruption-related risks arise from anticipated or unanticipated events that can impact an organisation's standard operating processes and cause significant immediate and long-term damage if no action is taken.

Therefore, it is crucial to have contingency plans and processes in place to:

- Respond and **Stabilise** the immediate impact of high risk disruptive events as soon as possible;
- Ensure **Critical Business Functions** can be recovered and continue;
- Facilitate the **Recovery** and return to a realistic and desired operating condition as soon as possible; and
- Capitalise on any **Opportunities** identified throughout the disruptive event.

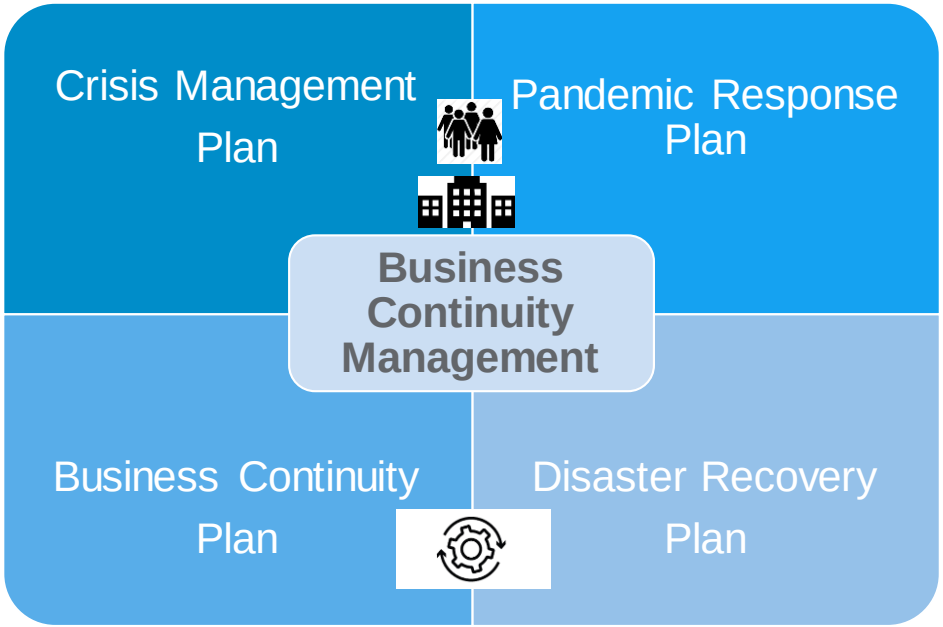
COVID-19 Business Continuity Management (BCM)

Since the emergence and rapid escalation of the COVID-19, businesses have been forced to expedite the development of BCM activities, regardless of whether a Business Continuity Plan has been in place.

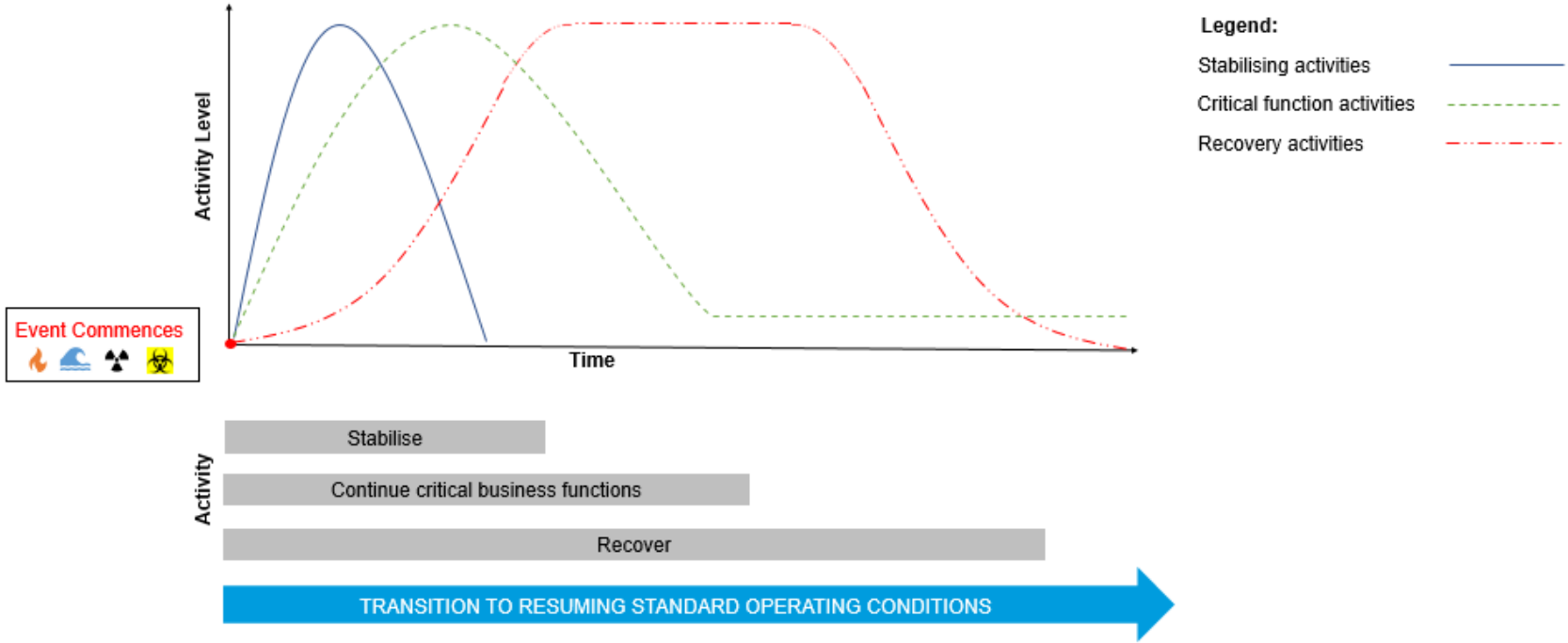
This has been to achieve the following:

- Prioritise the health and wellbeing of employees;
- Comply with all federal and state social distancing requirements;
- Fulfill customer agreements and additional requirements;
- Continue operating conditions to the highest degree possible; and
- Continuously adjust to the volatile foreign and domestic economic conditions.

Fundamentals of BCM

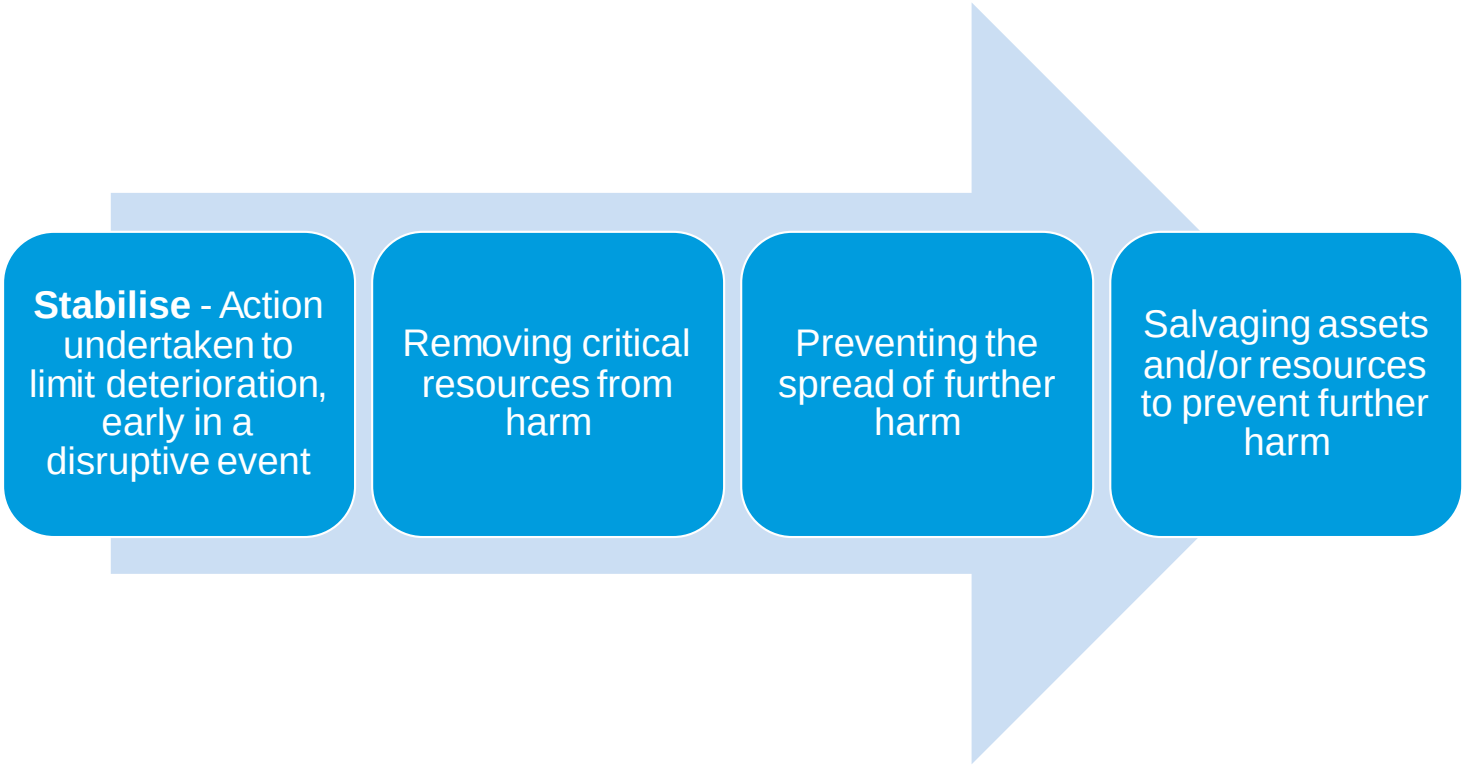


Fundamentals of BCM

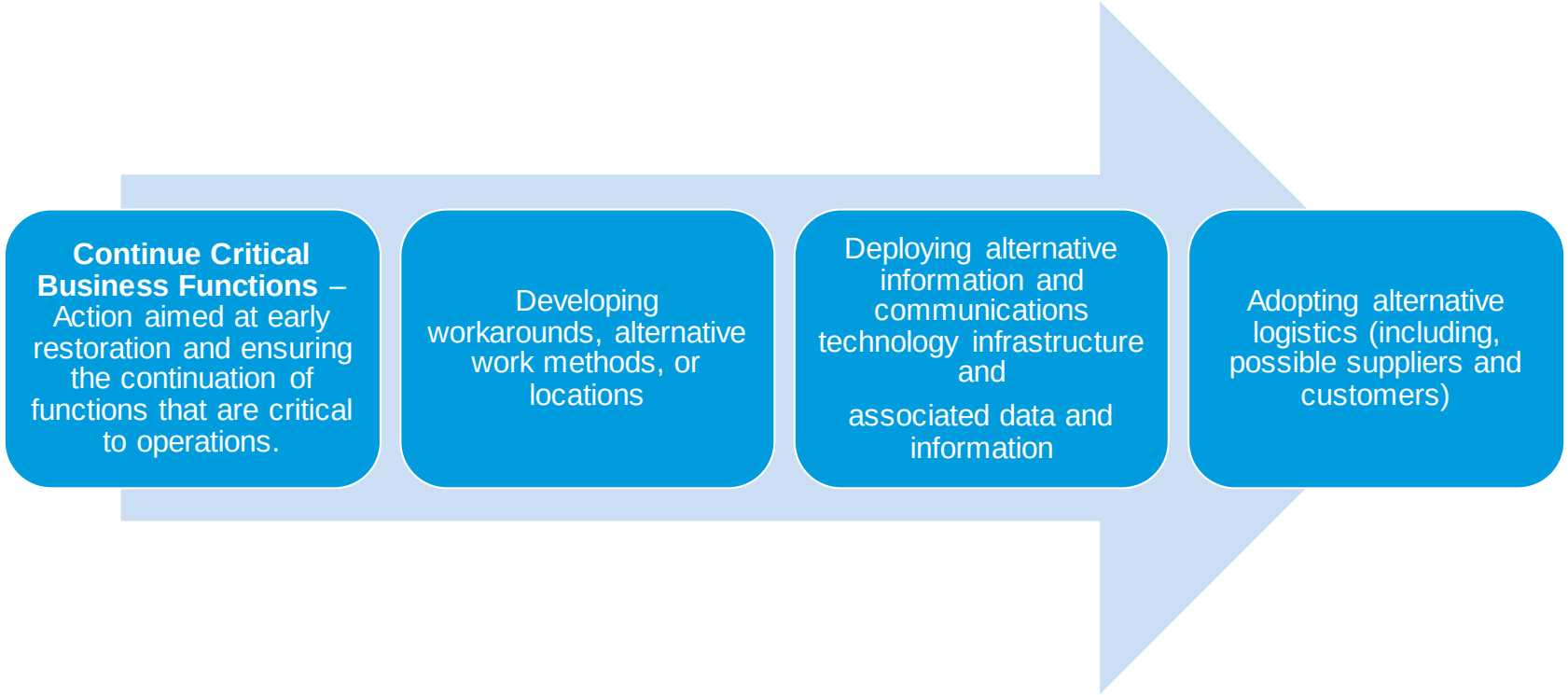


Source: AS/ANZ 5050:2010

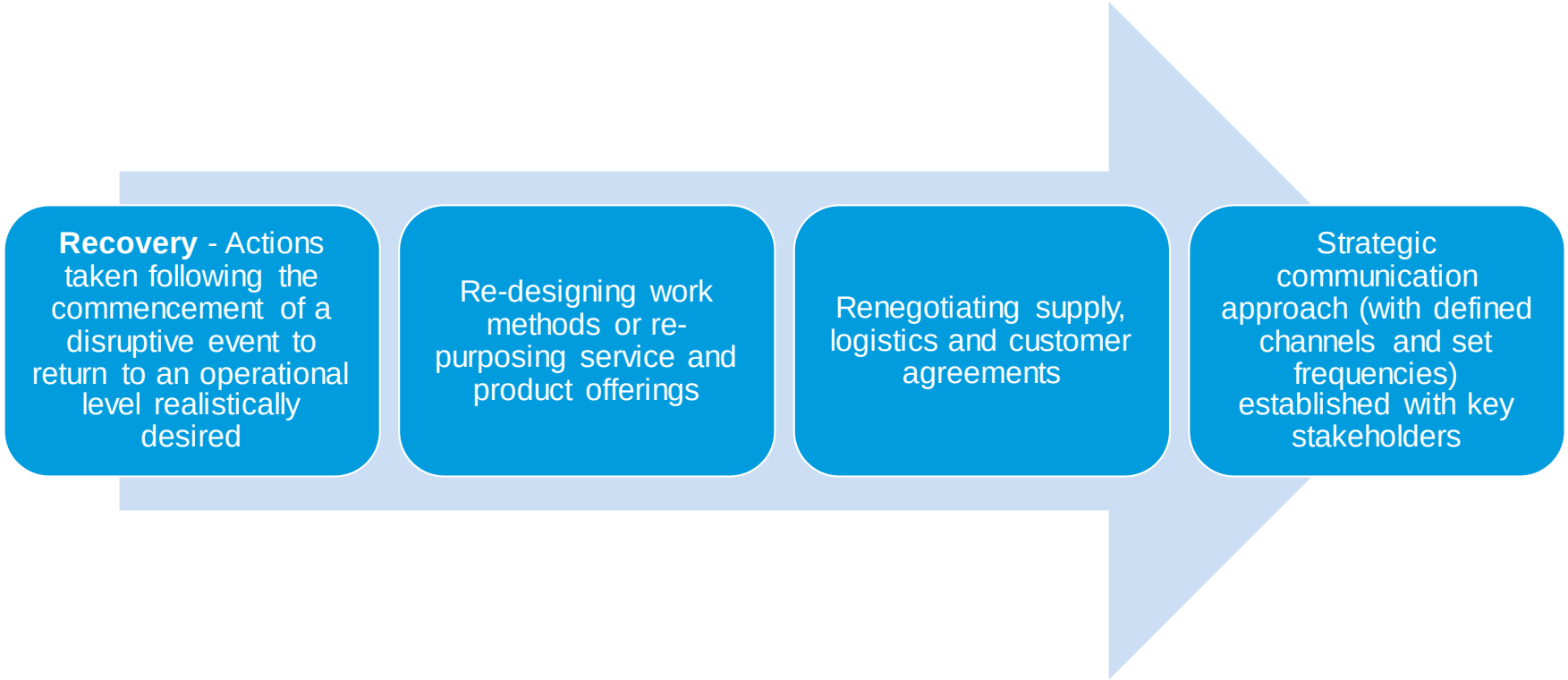
Fundamentals of BCM



Fundamentals of BCM



Fundamentals of BCM



Recovery Strategy Implementation and Monitoring

To effectively respond to the disruption of COVID-19, organisations have implemented a variety of rapid response recovery strategies:

- Working Remotely From Home;
- Diversifying Current Suppliers or Sourcing Alternative Suppliers;
- Reductions in Non-Essential Expenditure; and
- Furloughing Employees.

However, it is also important to identify and respond to the various business risks which are associated with the implementation of recovery strategies and foreign work processes

RSM

Recovery Strategy Implementation and Enhancements

Working Remotely From Home

Business Risks	Additional Control Mechanisms
Employee health and wellbeing	Expanded Employee Assistance Program with extra support and engagement mechanisms
Increased cyber security vulnerabilities	Additional cyber-security controls such as enhanced firewalls and anti-virus software, penetration testing, multi-factor authentication and reviewing system privileges
Productivity and efficiency losses are not detected	Revision of performance targets or how performance is measured. Implementation of tailored performance and productivity monitoring mechanism.
Fraud, corruption and reputational losses	To be covered in detail by Roger Darvall-Stevens

RSM

Recovery Strategy Implementation and Enhancements

Diversifying Current Suppliers or Sourcing Alternative Suppliers

Business Risks	Additional Control Mechanisms
Violation of existing contractual supplier agreements or breaching government procurement rules (or panel arrangements)	Reduce vulnerability by conducting a detailed review of existing supplier contracts and State or Federal Procurement Rules if a public sector organisation
Lack of continuous review of suppliers ability to supply given the increased market demand	Maintain frequent and honest communications with all critical suppliers to ensure that they are still capable of providing essential supplies at the required levels
Surplus supplies once the pandemic conditions and increased demand through '*panic buying*' decreases	Forecast the anticipated customer demand after the pandemic conditions have de-escalated and include an option to reduce minimum supply levels within all new supplier contracts

RSM

Recovery Strategy Implementation and Enhancements

Reductions in Non-Essential Expenditures

Business Risks	Additional Control Mechanisms
Lack of capitalisation on market opportunities and conditions	Regular environmental scanning to identify marketing opportunities and allocate resources where appropriate
Lack of innovation and continued improvement opportunities	Allocation of available or underutilised staff resources to focus on innovative opportunities where appropriate
Ongoing conflict when defining and separating ‘essential’ and ‘non-essential’ activities and expenditures	Continued utilisation of consistent communications and rational explanations for all difficult business decisions

Recovery Strategy Implementation and Enhancements

Furloughing Employees

Business Risks	Additional Control Mechanisms
Permanent loss of talented employees to competitors or different industries	Confidential identification and prioritisation of the retention of high-performing and talented employees
Increased employee anxiety and fear of potential job losses	Open, honest and reassuring communications to employees regarding the organisations approach to protecting jobs and the potential need to furlough employees
Potential accusations of preferential treatment	Active monitoring of employee cohesion and complaints registered to identify any potential conflict
Potential violation of employment rights and privileges.	Thorough assessment of all enterprise agreements and employee rights and privileges before making any decisions on furloughing employees or reducing hours

RSM

Time-Based Scenarios for Continuous Monitoring

Whilst the rapid emergence and escalation of the COVID-19 global pandemic has expedited the development and implementation of a variety of recovery strategies, it is imperative that these strategies are monitored considering the current uncertainty of time.

The benefits of utilising time-based scenario monitoring includes the following:

- Understanding of the best and worst case impact to the organisation;
- The risks associated with the chosen recovery strategies over time; and
- Escalation points for the development or implementation of new recovery strategies that are contingent on time.

Time-based Scenario Monitoring

Medium-Term (2-6 months)

- **Employee Health and Wellbeing** - Has your business identified all potential health and wellbeing requirements for its employees and prioritised the provision of resources and support to enable them to continue working in the challenging environment?

- **Sustainability of short-term workarounds:** Can recovery strategies developed be relied upon for 3 to 6 months? Is there a need for further investment and allocation of resources to develop medium to long term strategies if the pandemic were to continue longer?

Long-Term (6-12 months)

- **Strategic Objectives:** Are the strategic objectives of the business still achievable or is a review and refresh required to guide the immediate and long-term decision making if the disruption from the pandemic will continue through 12 months?

- **Financial sustainability:** Consideration of sustained impact of the pandemic on the national economy if the disruption where to continue through 12 months, and the potential for further disruption events not considered in a short or medium term scenario. E.g. key customer not at risk in the short – term, but perhaps in the long-term.

RSM

Resources

Key best practice guidance and resources:

- AS/NZS 5050:2010: *Business Continuity – Managing disruption-related risk*
- AS ISO 22301:2017: *Societal Security – Business continuity management systems*

COVID-19: FRAUD AND CORRUPTION AND WFH CYBERFRAUD / SECURITY RISKS

Roger Darvall-Stevens, Partner and National Head of Fraud and Forensic Services, RSM Australia

RSM

What we will cover

- Why be alert, not alarmed for fraud, corruption and workplace misconduct
- Understanding why it occurs in these crisis times (GFC, natural disasters, and now COVID-19)
- Known occurring COVID-19 fraud and similar scams, including cyberfraud
- What can businesses do, including WFH risk mitigation

RSM

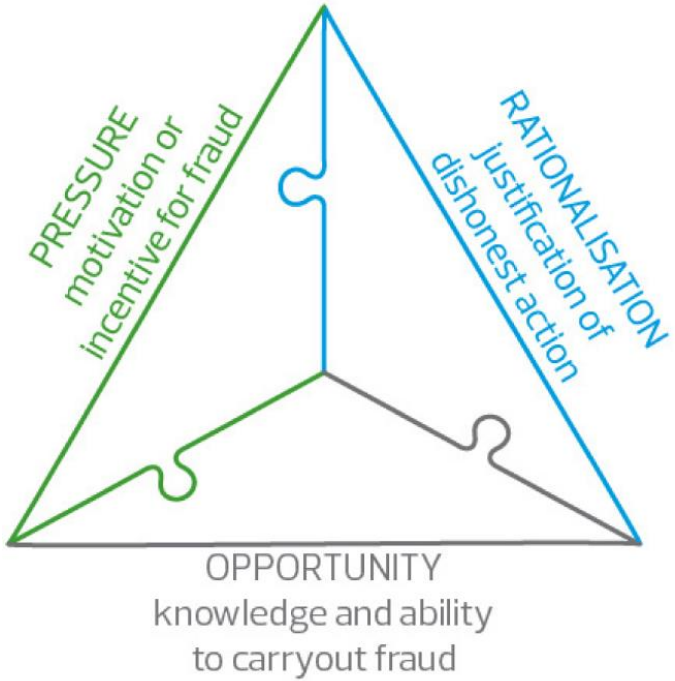
Why be alert, not alarmed, for fraud, corruption and workplace misconduct

- What do we know from COVID-19 similar global crisis events (e.g. 2008 GFC, and natural disasters)?
  - Fraudster will prey on business and individuals in times of crisis, hoping that usual internal control defences are lax
  - Internal controls may be circumvented for expediency to keep business processes operating or govt. assistance to private sector
  - Management review may not be as vigilant due to distraction by COVID-19 and other management responsibilities
  - The fraud triangle is the best insight to the circumstances leading to fraud, corruption and workplace misconduct

RSM

Understanding why it occurs in times of crisis

- First espoused by criminologist Dr Donald R. Cressey in the 1950s
- Still just as relevant today
- All 3 elements must be present for fraud, corruption or improper conduct to occur in crisis times:
  - **Motivation** through financial stress / hardship / job loss fear
  - **Rationalisation** that "I deserve it / extra money due to my hard work or loyalty"
  - **Opportunity** as internal controls or management review are not vigilant or diligent



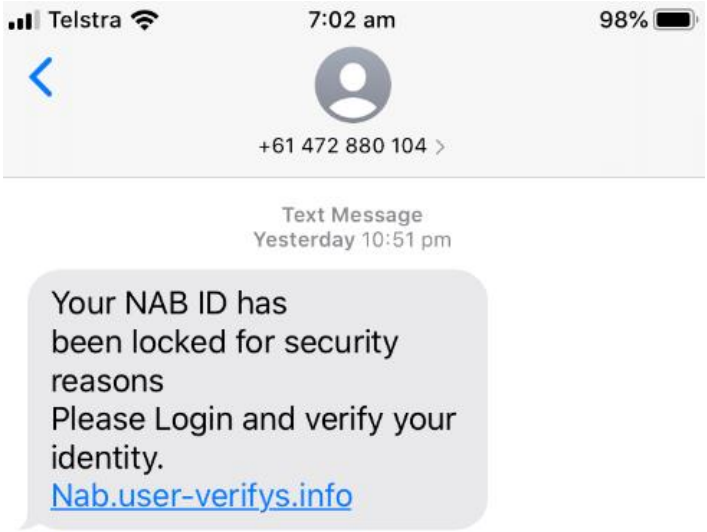
Known occurring COVID-19 fraud and similar scams

- Outright theft and obtaining fraudulent benefits
- Cyberfraud/security scams - ‘phishing’ (via email), ‘vishing’ (via voice by ‘phone), ‘smishing’ (via text), ‘pharming’ via installing malicious code into a PC though clicking on a link etc.
  - i.e. purporting to be from reputable companies to induce confidential / private information release without authorisation, PC virus infection, etc.)
- Investment scams
- Counterfeit or non-existent COVID-19 equipment
- Fake online shopping sites requesting unusual payment methods
- Unsolicited Coronavirus related emails

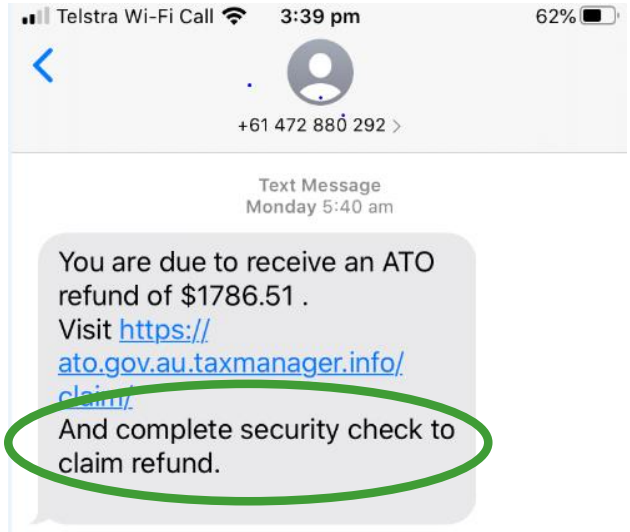
RSM

Known occurring COVID-19 fraud and similar scams

Smishing examples attempted on Roger (presenter)



Roger's response: "*That's great but I don't have a nab account!!!*"



Roger's response: *"WTF (What The Fraud!) – No, I don't think so!!!"*

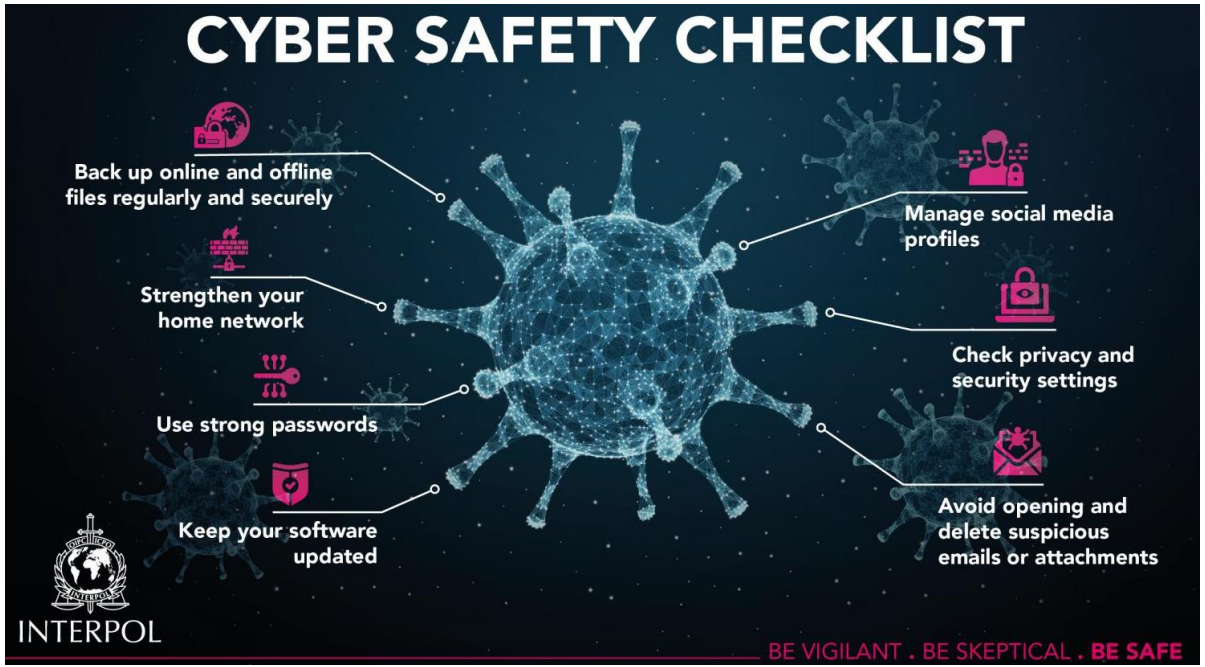
Known occurring COVID-19 fraud and similar scams

- Scams to organise the early release of superannuation
- False vendors
  - e.g. some great tips in NSW ICAC's 'Managing Corrupt Conduct During the COVID-19 outbreak' (April 2020)
- Employees WFH (a risk to be aware of is considerable amount of the 'work time' being spent on non-employer related activities)
  - Ensure IT / cyber security measures are up-to-date like virus protection, firewalls, security patches etc. and follow your IT policy / advice
  - Be careful of security weaknesses (e.g. Zoom video conferencing security weakness - can expose Windows user names & passwords to attackers when malicious links are clicked in a chat window)
  - Watch what is in the background of your video conferencing (photos, identity documents, etc.)
  - Be wary for unidentified meeting participant(s)

RSM

Known occurring COVID-19 fraud and similar scams

An example – INTERPOL's Cyber Safety Checklist



Source: courtesy of INTERPOL, Doug Witschi from Cybercrime Threat Response

RSM

What can businesses do including WFH risk mitigation

- Stay ever vigilant and diligent focussing on compliance, internal & external audit, & internal controls testing & strengthening
- Do not ignore or reduce your GRC requirements or practices
  - e.g. don't let your whistleblower program be ineffectual
- Provide employees with tips & traps of which to be aware to avoid being a victim personally of COVID-19 fraud scams, which translates to being more alert in daily work duties
- Consider conducting a COVID-19 anti-fraud/corruption and workplace misconduct review
- Do not forget about upskilling or continuous CPE development
  - e.g. CFE (Certified Fraud Examiner) Course

RSM

Anti-fraud training / global CFE certification

RSM is the exclusive Authorised Trainer in Australia for the global ACFE (Association of Certified Fraud Examiner) CFE (Certified Fraud Examiners) Exam Review Course – now virtual until in-person can be re-instated

- Investigation
- Law
- Financial Transactions and Fraud Schemes
- Fraud Prevention and Deterrence

RSM

Contact us

Roger Darvall-Stevens

Partner, National Head of
Fraud & Forensic Services

RSM Australia

T 0421 056 683

roger.darvall-stevens@rsm.com.au

www.rsm.com.au

Milind Sheth

Senior Manager,
Fraud & Forensic Services

RSM Australia

T 0430 114 461

milind.sheth@rsm.com.au

www.rsm.com.au

Questions and answers?

Thank you for your time and attention.

The latest information and webinar details can be found at:
rsm.com.au/coronavirus

THE POWER OF BEING **UNDERSTOOD**

RSM.COM.AU