BDO AND IPAA ‘RETHINK’ INFORMATION SERIES

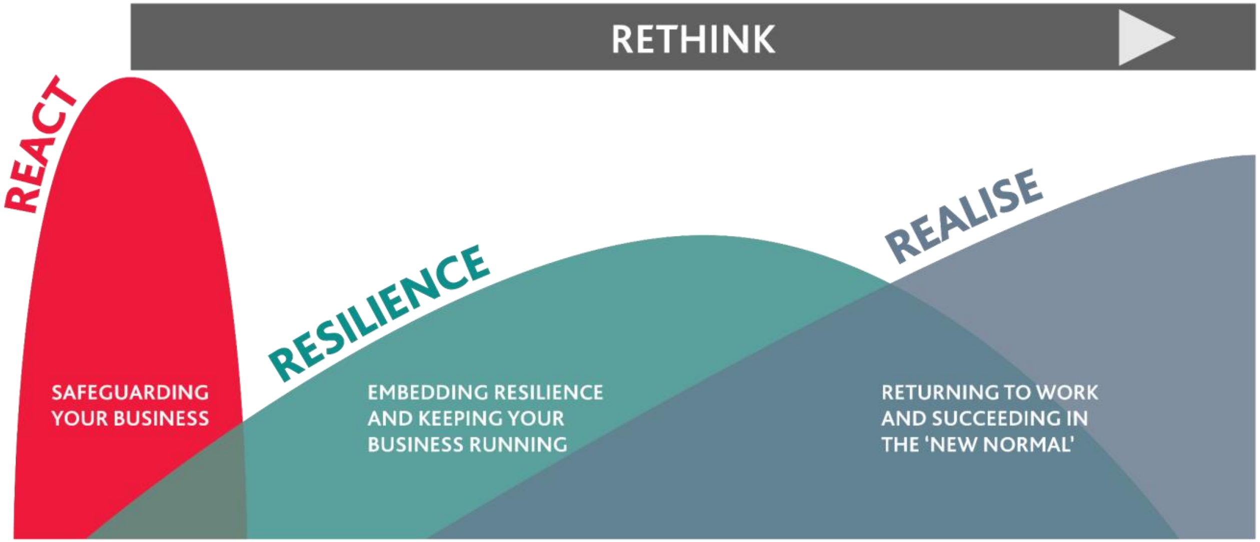
CYBER SECURITY AT THE EXECUTIVE LEVEL

September 2020

HELPING ORGANISATIONS BOOST THEIR ORGANISATIONAL RESILIENCE

In the current operating climate, knowing how to plan for ‘what’s next’ is crucial. To help guide this process BDO has drawn on the first-hand experience and insights of its global teams to develop the ‘Rethink’ framework. Much of the world has moved past the react phase, and is heavily entrenched in resilience, where the goal is to identify what will help your organisation be successful in the new normal.

A focused effort to embed improvements and risk mitigation approaches in this Resilience phase — made up of five key focus areas — is what will set an organisation up for success in the ‘new normal’.


RETHINK
REACT
SAFEGUARDING YOUR BUSINESS
RESILIENCE
EMBEDDING RESILIENCE AND KEEPING YOUR BUSINESS RUNNING
REALISE
RETURNING TO WORK AND SUCCEEDING IN THE ‘NEW NORMAL’

The way in which businesses respond to the initial impact of the COVID-19 crisis, minimising the catastrophic effects on its business operations, employee safety, supply chain and ongoing financial viability.

Maintaining business operations during disruption using techniques that allow people, processes and information systems to adapt to changing patterns. The ability to alter operations in the face of changing business conditions preserving the continuity of the provision of ‘critical functions’ to a firm's customers.

Applying the learnings from key resilience activities and continuing to adapt. Successfully adapting to new business models and ways of working are needed to address essential and obligatory political, economic, socio-cultural, and technological changes.

BDO AND IPAA's 'RETHINK' INFORMATION SERIES

This Information Series focuses on five of the critical enablers of the Resilience phase, which are particularly relevant for public sector organisations. We will guide you through the role each can play in the decision making process and the important factors your leaders must consider as they look to the future.

If you would like more information about BDO's Rethink framework, please visit our website for material and podcasts covering a wide range of topics, including people, operations, compliance, risk, and finance.

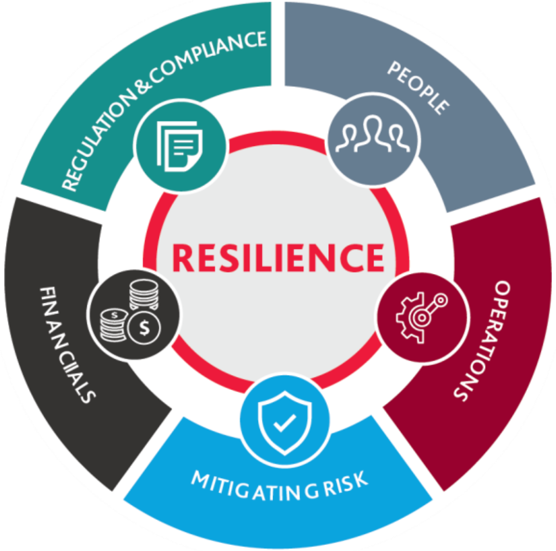
CYBER SECURITY AT THE EXECUTIVE LEVEL

DIGITAL TRANSFORMATION

REIMAGINING BUSINESS MODELS

RELIABLE INFORMATION AT THE EXECUTIVE LEVEL

WORKFORCE TRANSFORMATION



CYBER SECURITY AT THE EXECUTIVE LEVEL

RAPID CHANGES GIVE RISE TO CHALLENGES

Senior management and operational teams have faced many dilemmas recently when considering how to continue operations while addressing changes to the organisation's services, workforce planning and supporting technology.

CHANGES

- Increase in remote working has created a hybrid workforce for organisations to manage securely
- Customer engagement channels/methods are occurring in a virtual setting
- Increased use of personal devices by employees to conduct business transactions
- Increased reliance on collaboration tools to maintain internal and external engagement
- New trends and patterns of end-users and employee behaviour
- Cyber security threat actors taking advantage of the changes and the challenges faced

CHALLENGES

People

- Workforce models are changing to reflect a hybrid working environment
- Key person/team dependencies are required to support environments
- Management is not getting timely insights on the emerging/changing cyber threat landscape
- Increased reliance on the awareness of employees to protect information and systems

Processes

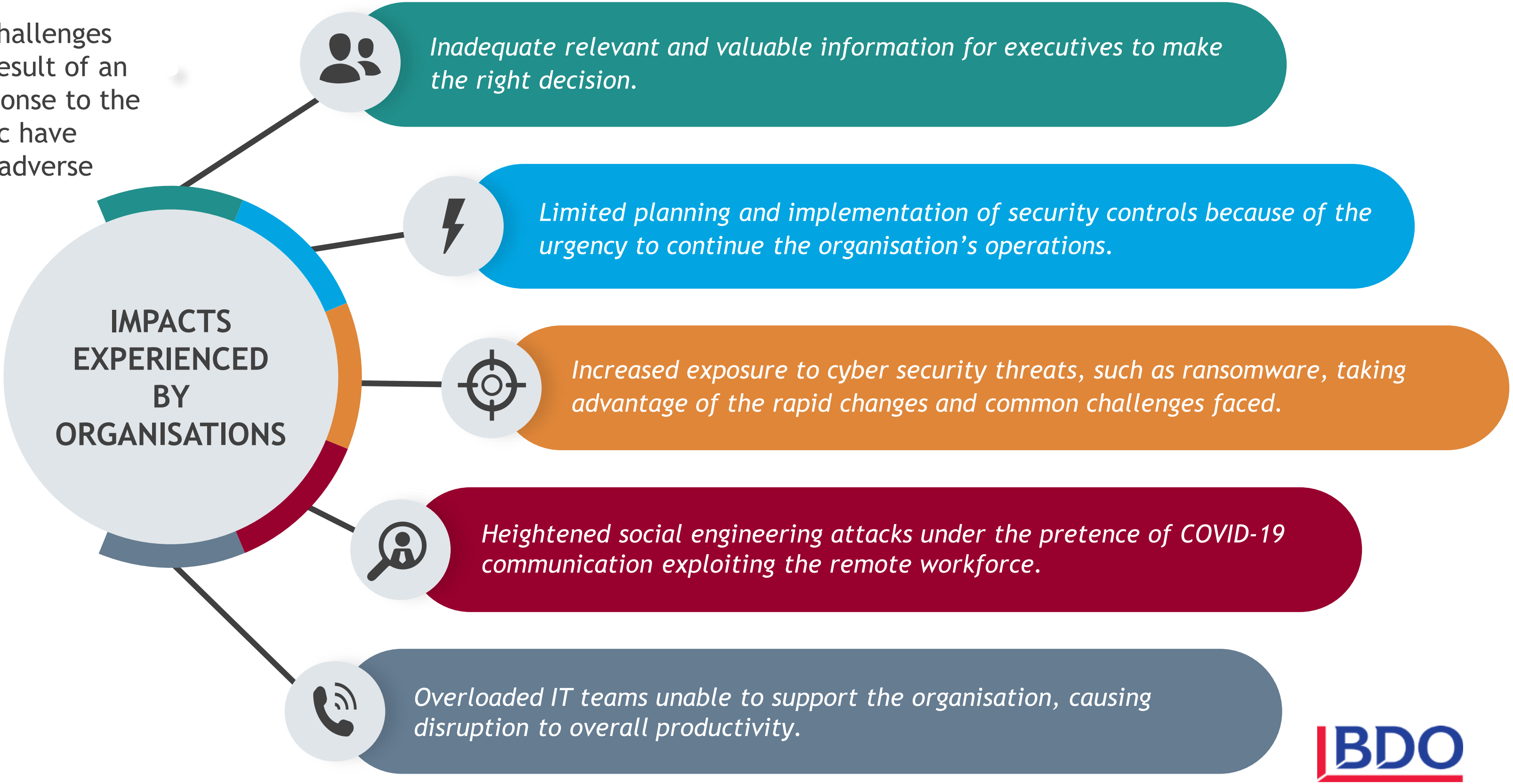
- Increased IT/help desk requirements to support remote workforce
- Limited preparation of business continuity plans
- Limited understanding of supply chain risks
- Delivery of services through different channels
- Policies and procedures are no longer relevant to services delivered remotely and digitally

Technology

- Increased reliance on technology to support virtual working environment (e.g. collaboration)
- Rapid adoption of new technology with limited time to assess risk exposures.
- Rapidly changing technology landscape impacting user identity and access management controls
- Limited visibility and control over measures adopted to secure end user environments

THE IMPACTS OF THESE CHALLENGES

The changes and challenges experienced as a result of an organisation’s response to the COVID-19 pandemic have caused significant adverse impacts to many.



IMPACTS EXPERIENCED BY ORGANISATIONS

Inadequate relevant and valuable information for executives to make the right decision.

Limited planning and implementation of security controls because of the urgency to continue the organisation’s operations.

Increased exposure to cyber security threats, such as ransomware, taking advantage of the rapid changes and common challenges faced.

Heightened social engineering attacks under the pretence of COVID-19 communication exploiting the remote workforce.

Overloaded IT teams unable to support the organisation, causing disruption to overall productivity.

BDO

LESSONS LEARNED TO UPLIFT MATURITY

Responding to the COVID-19 pandemic has tested the existing cyber security controls of many organisations. This has unearthed deficiencies and weaknesses that many organisations can address to protect against continually evolving threats and attacks.

Key lessons learned

- Organisations that have supported work from home arrangements prior to the COVID-19 crisis have typically not required significant changes to business processes and infrastructure to achieve a sound internal control environment. Conversely, those that have needed to rapidly modify operating processes or infrastructure now must fully consider the impact on cyber security
- Increased remote collaboration requires the use of supporting applications and technology. These collaboration platforms may have sub-optimal cyber security controls. Organisations must identify and test preferred collaboration platforms
- Demand on IT helpdesk/support has increased because of the workforce's limited knowledge of new systems and applications. Organisations must develop supporting processes, training content and easy-to-follow checklists uplift security awareness when working remotely
- Contract management has become critical to ensuring organisations receive goods and services in a timely way, safely and to the expected quality. Organisations need to increase due diligence processes to ensure suppliers remain reliable and viable
- Organisations have evolved workforce planning processes with significant variability. To reduce the risk to operations, organisations should identify critical resources (employees and contractors), along with contingencies to ensure they remain separated
- With less people based on sites, physical access security controls need to be increased, such as deploying monitoring capabilities
- Executives and boards require a better understanding of the holistic cyber security context. Organisations need to align their information and cyber security approach with business impacts and risks to provide relevant and concise information to decision makers

THE OPPORTUNITY TO UPLIFT MATURITY

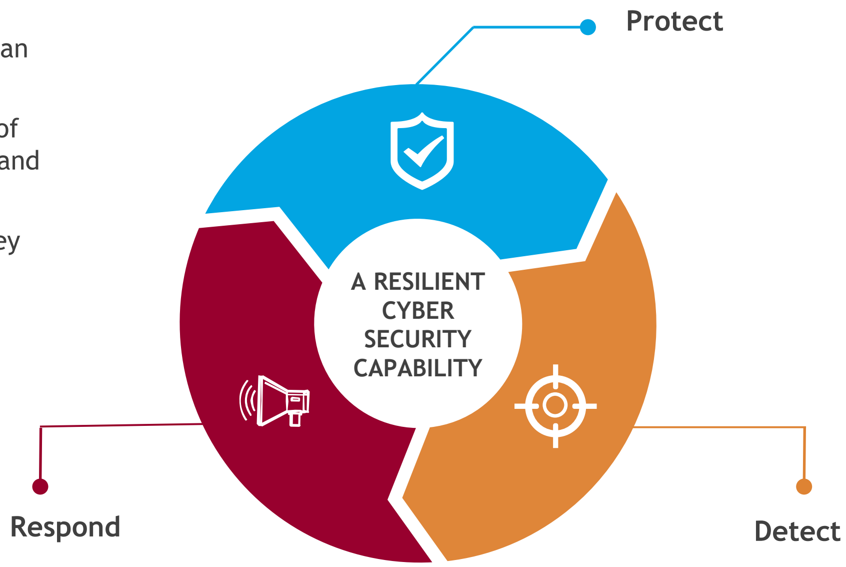
Lessons learned have highlighted areas for improvement to ensure organisations address the new normal.

The new normal of a hybrid workforce, agile technologies, and changing organisational functions requires a resilient cyber security capability that can keep up with the continuously evolving threat landscape.

A resilient capability addresses cyber security proactively through a series of controls of people, processes, and technology, layered to mitigate threats and protect valuable information and systems.

Throughout the COVID-19 pandemic response, we observed the following key controls that organisations were reactive in approaching:

- Workforce planning
- Employee awareness and knowledge
- Risk assessment of changing remote working environment
- Third-party/supplier management
- Identity and access management
- Understanding changing threat environment
- Response and recovery plans.



PROACTIVE APPROACH TO ESTABLISH RESILIENCE

Key controls of people

Protective controls	Observation	Recommendations
Workforce planning	The risk associated with filling critical roles was increased during the height of the COVID-19 response period. The importance of simplifying workflows and performing contingency planning was also amplified. Organisations that operated in industries controlling critical infrastructure were generally prepared and had critical role contingency plans in place. However, it was observed across other industries that there had been little planning to understand the impacts should critical roles be affected. From a cyber security perspective, critical roles may include those monitoring systems, performing system upgrades, or maintaining network capacity/connectivity.	• Perform workforce planning to identify critical cyber security roles • Establish contingency plans to mitigate the impact of the loss of staff to perform those critical roles • Develop a program to upskill and train other staff to fulfil critical roles in emergency situations • Augment your critical teams with external support when required
Employees awareness and knowledge	Increase in remote working increases an organisation's exposure to cyber security threat actors. This was particularly evident at the start of the COVID-19 pandemic, as there was an increase in phishing and Business Email Compromise (BEC) attacks looking to exploit weaknesses in work flows and process changes. Organisations that have supported work from home arrangements prior to this current crisis have typically not required significant changes to business processes and infrastructure to achieve a sound internal control environment. Those that did not were not prepared for large-scale remote working and often relied to staff using personal devices to connect to their organisation's network and operate in an environment not set-up with internal controls to support remote working.	• Organisations sign-up to the Australian Stay Smart Online program to ensure that are aware of the latest cyber threats • Establish work from home guidelines and educate staff on how to follow these • Establish a security awareness and training program to ensure staff are aware of the increased cyber threat environment to their organisation • Regularly brief management on the changing cyber threat landscape • Ensure your IT helpdesk is appropriately trained and educated on emerging cyber threats and how to support staff with these • Regularly monitor the results of the above to ensure management and staff are sufficiently prepared for the cyber threat environment

PROACTIVE APPROACH TO ESTABLISH RESILIENCE

Protective control	Observation	Recommendations
Risk assessment of changing remote working environment	The COVID-19 response saw organisations experience unexpected growth and delivery of services through different channels, which may not have been appropriately planned for. Organisations integrated new technologies and software into their environments to cope with the demand and changes, especially in the way staff collaborated internally and engaged with customers externally. Additionally, the changed work postures and technologies created pressure on IT services to cope with increased demand of service requests to support these.	• Perform capacity planning as part of the overall Business Continuity Plan and involve the IT and cyber security teams early • Establish a cyber security risk and change management process to ensure new technologies and software are appropriately integrated and implanted in the organisation • Understand cyber security risks and postures of your third party providers and supply chain • Identify the key controls required to protect your digital and information assets against relevant threats to the environment and test the operational effectiveness of these • Align the risks with business objectives and assess risks by considering impacts to the organisation • Ensure the executive team knows the risks and understands the holistic security context to make informed decisions

PROACTIVE APPROACH TO ESTABLISH RESILIENCE

Protective control	Observation	Recommendations
Third-party/supplier management	The COVID-19 pandemic exposed supply chain issues that impacted the ability of organisations to effectively deliver services to their staff and clients. There was a reliance on third parties to manage their own changing working environment without validating it. This created a lack of understanding about the overall risks in many organisations' supply chains.	• Meet with your organisation's third parties/service providers to understand and assess the processes they have put in place to support with working from home arrangements • Define baseline cyber security standards for your organisation's third parties and supply chain to comply with • Review and assess the maturity of your organisation's suppliers to determine if their capabilities and experience align with baseline security requirements • Ensure third party and supplier contracts include specific security and availability requirements (not just standard clauses) for the service provided This includes: – Service level agreements, response times, escalation requirements, and notifications for planned and unplanned outages – The right for your organisation to carry out an audit, risk assessment, or penetration test to assess controls and capabilities managed by the vendor – Clear and specific data ownership – Contract termination terms, such as time to support transitioning data to another vendor and the format of data to be provided – Communicating your organisation's security policies to suppliers.

PROACTIVE APPROACH TO ESTABLISH RESILIENCE

Key controls of people and processes

Responsive control	Observation	Recommendations
Response and recovery plans	Coordination issues during the response and recovery phases of an incident are amplified during an event like the COVID-19 pandemic. Many organisations maintained the same work flows despite changes to the roles and responsibilities of staff operating in a remote working environment. There was generally a lack of understanding regarding the impact of how remote working may change the efficiency and flow of reporting (e.g. time, means). It was also observed that recovery plans and procedures were outdated, not detailed and/or exercised.	• Establish a business continuity strategy or plan that informs other detailed procedures, such as disaster recovery and incident response • Assign accountabilities and responsibilities to manage, update and operate the plans. Ensure these include a remote working environment • Ensure there is a multi-disciplinary team approach to response and recovery (not just IT focussed) • Ensure appropriate training/awareness is provided to staff about their responsibilities during an incident and how they should be using the plans • Rehearse and test the plan for its effectiveness • Capture the lessons learned and update the plan as appropriate

PROACTIVE APPROACH TO ESTABLISH RESILIENCE

Key controls of process and technology

Protective and detective control	Observation	Recommendations
Identity and access management	Organisations that had experience with facilitating remote working generally had appropriate network, system and application controls in place. Conversely, those that had not did not fully appreciate the potential impacts and were more exposed to the increased risk of cyber attacks. Many organisations did not appropriately strengthen identity access management controls (privileged and user) to mitigate the increase risk of unauthorised access.	• Develop an enterprise wide user access management standard that is based on user roles • Ensure system access accounts are granted rights and privileges only if required to perform their functions • Continually review accounts and adjust rights and privileges as required • Monitor access and setup automated notifications for unusual and critical behaviour • Deploy Multi Factor Authentication (MFA) for all privileged accounts to critical applications • Deploy MFA for all remote access to corporate network • Adopt password guidelines recommended by the National Institute of Standards and Technology in publication 800-63B (Digital Identity Guidelines)

PROACTIVE APPROACH TO ESTABLISH RESILIENCE

Key controls of process and technology

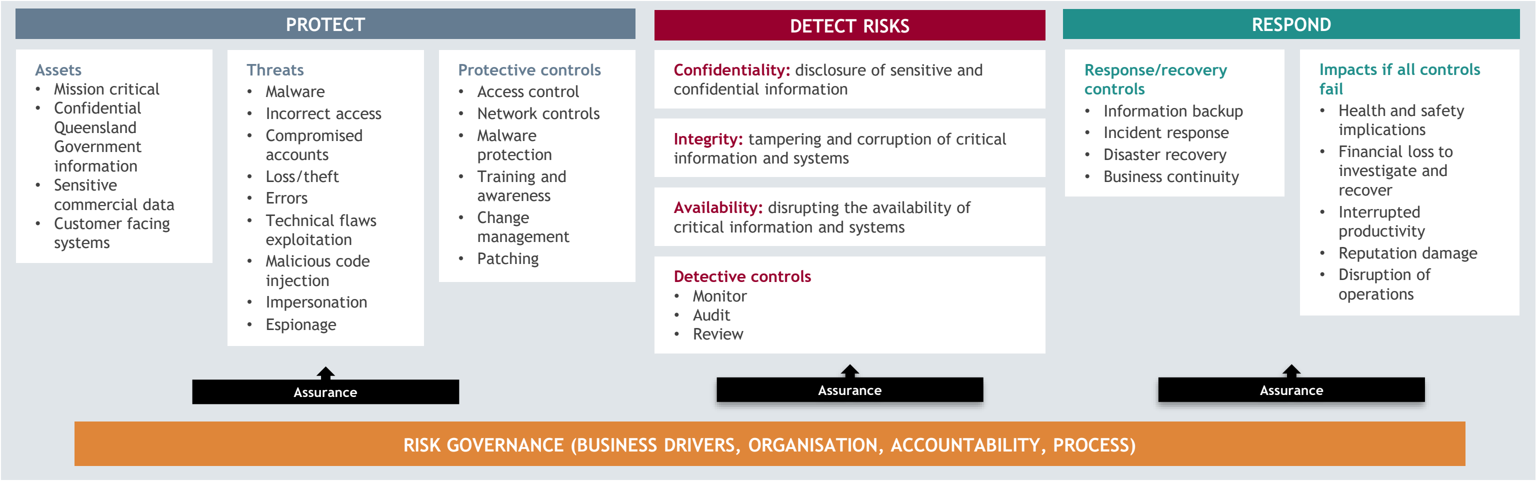
Protective and detective control	Observation	Recommendations
Understanding changing threat environments	The changes in working environments meant some organisations were underprepared to facilitate staff working from home with secure devices. There was also an increase in the use of personal devices and the implementation of unsanctioned applications to support team collaboration when working from home. These changes expanded the organisations' technology footprint and increased the likelihood of threat events (malicious and accidental) associated with data and regulatory breaches.	• Perform regular threat briefings at all levels of the organisation • Supply staff with safe user guidelines to ensure they work in a cyber safe environment when working from home • Perform contingency planning that covers the allocation of corporate devices based on risk (this should include procurement requirements) • Consider deploying a mobile device management solution to enforce minimum security requirements and restrictions on enrolled devices

THE WAY FORWARD

Today's continually evolving cyber security landscape requires an approach that maintains visibility over changes, indicates risks clearly, and adjusts rapidly and steadily.

Our recommendations for a repeatable cyber security risk management process to continually uplift your organisation's maturity are:

- Identify the assets that need protecting by assessing the impact of compromise to your organisation
- Have visibility over your organisation's threats, as well as the likelihood and applicability to your critical assets
- Implement your organisation's controls and test the effectiveness and adequacy against threats identified
- Monitor your risks by continually reviewing your assets, threats and controls, and their effectiveness to minimise the risks
- Align your risks and impacts with business objectives to clearly communicate the risks to decision makers.



PROTECT

Assets
- Mission critical
- Confidential Queensland Government information
- Sensitive commercial data
- Customer facing systems

Threats
- Malware
- Incorrect access
- Compromised accounts
- Loss/theft
- Errors
- Technical flaws exploitation
- Malicious code injection
- Impersonation
- Espionage

Protective controls
- Access control
- Network controls
- Malware protection
- Training and awareness
- Change management
- Patching

DETECT RISKS

Confidentiality: disclosure of sensitive and confidential information

Integrity: tampering and corruption of critical information and systems

Availability: disrupting the availability of critical information and systems

Detective controls
- Monitor
- Audit
- Review

RESPOND

Response/recovery controls
- Information backup
- Incident response
- Disaster recovery
- Business continuity

Impacts if all controls fail
- Health and safety implications
- Financial loss to investigate and recover
- Interrupted productivity
- Reputation damage
- Disruption of operations

RISK GOVERNANCE (BUSINESS DRIVERS, ORGANISATION, ACCOUNTABILITY, PROCESS)

CONTACT US

JASON SORBY
National Lead Partner, Consulting
+61 7 3173 5506
jason.sorby@bdo.com.au

LEON FOUCHE (author)
Partner, Cyber Security
+61 7 3237 5688
leon.fouche@bdo.com.au

This publication has been carefully prepared, but it has been written in general terms and should be seen as broad guidance only. The publication cannot be relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact the BDO member firms in Australia to discuss these matters in the context of your particular circumstances. BDO Australia Ltd and each BDO member firm in Australia, their partners and/or directors, employees and agents do not accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

BDO refers to one or more of the independent member firms of BDO International Ltd, a UK company limited by guarantee. Each BDO member firm in Australia is a separate legal entity and has no liability for another entity's acts and omissions. Liability limited by a scheme approved under Professional Standards Legislation.

BDO is the brand name for the BDO network and for each of the BDO member firms.

BDO