August 2024

Governance Institute of Australia

THOUGHT LEADERSHIP GUIDE

Effective Cyber **Risk Management**

A best practice governance guide for digitally secure and resilient organisations

Table of Contents

1. About us

A national membership association, Governance Institute of Australia advocates for a community of governance and risk management professionals, equipping over 8,000 members with the tools to drive better governance within their organisation. We tailor our resources for members in the listed, unlisted, not-for-profit, and public sectors, and ensure our member's voice is heard loudly. As the only Australian provider of chartered governance accreditation, we offer a range of short courses, certificates, and postgraduate study to help further the knowledge and education of the fast-growing governance and risk management profession. We run a strong program of thought leadership, research projects and news publications and draw upon our membership of the Chartered Governance Institute to monitor emerging global trends and challenges to ensure our members are prepared. Our members know that governance is at the core of every organisation — and in these tumultuous times, that good governance is more important than ever before.

Acknowledgements

Written by Francesca Dickson FGIA FCG, Chair of the Governance Institute of Australia Risk and Technology Committee. Governance Institute acknowledges the valuable contributions of the Risk and Technology Committee members Dr Marcos Tabacow FGIA, Ben Lester FGIA, Robbie Sinclair FGIA, Teresa Riccio-Goodwin FGIA, Tim Timchur FGIA FCG, Chirag Joshi of 7 Rules Cyber and Governance Institute staff Catherine Maxwell FGIA FCG, GM Policy and Advocacy and Daniel Popovski, Senior Policy and Advocacy Advisor.

2. Foreword

Cybercrime is a complex global challenge that is increasing in frequency and sophistication impacting most people and organisations. We can all relate to a cyber incident affecting us or people we know. Whether it's a suspicious email, unsolicited text message, or notification of a service provider outage, the persistent threat sits amongst us at work, at home and throughout our daily lives. The Australian Institute of Criminology, Cybercrime report found that 47 per cent of respondents experienced at least one cybercrime in the 12 months prior to the survey and the Australian Cyber Security Centre now reports on receiving a cybercrime report every seven minutes.

It is critical at a time of heightened geopolitical tensions, global economic uncertainty and increasing cybercriminal activity that Australian businesses remain aware and vigilant of the ongoing threat of cybercrime. As recent high-profile cyber incidents have demonstrated a significant cyber incursion can lead to substantial financial, legal and reputational costs to a business. However, cybercrime is not just a big business issue. It can impact small operators including family-owned enterprises. We are now witnessing a growing number of cybercriminals targeting small and medium-sized enterprises as a back door to large business supply chain networks. Yet Australian SMEs which make up 98 per cent of all businesses in Australia, spend less than $500 on cyber security annually and are less likely to ever fully recover after experiencing a major cyber incident.

Best practice cyber risk management for businesses large or small starts with good governance. This publication has been prepared by and for risk managers and governance professionals and business operators seeking to understand how to prepare, defend and respond to cyber incidents within their organisation and throughout their supply chain. The Guide aims to empower business leaders with practical frameworks and resources to adopt and apply best practice governance for a more secure and resilient organisation.

I am confident that the Guide will better prepare you to operate a more secure, digitally enabled organisation. No matter what your level of digital maturity, the Guide acts a useful step towards preparing for and creating a more resilient and cyber-secure organisation.

Megan Motto
CEO
Governance Institute of Australia

3. Introduction

The cyber risk landscape

Managing cyber risks is an essential element of good governance. Threats such as data theft, extortion and cyber-related operational disruption are increasing in Australia and globally, creating financial, legal, operational, and reputational impacts on business, government, not-for-profits, and individuals. The increased impact and urgency of cyber threats has also elicited a regulatory response and regulatory priorities in the areas of privacy legislation, critical infrastructure, and enforcement.[1]

Globally, 'cyber insecurity' remains a top-five risk in the World Economic Forum's Global Risk Report 2024.[2] The average annual cost of cybercrime is expected to increase from $8.4 trillion in 2022 to more than $23 trillion in 2027, with the Asia-Pacific region experiencing a huge increase in cyberattacks compared to its global counterparts.[3]

Several factors are driving an increased volume and sophistication of cyber-attacks. The increased uptake of remote work during the COVID pandemic and the continuation of hybrid working in many organisations, increasing uptake of collaboration platforms and tools such as video conferencing, cloud storage and file-sharing is rapidly shifting the boundaries of organisations' attack 'surface' that needs to be protected.

With increasing risks and incidents there is a growing recognition that cyber risks are business risks, and all leaders need to understand the cyber risk landscape. Cyber risk management is now everyone's business.

Why this guide?

This Guide has been developed for those who need to understand cyber risk management both at a holistic and practical level. This includes organisational decision-makers, directors, managers and others tasked with developing, implementing, evaluating or endorsing cyber risk management frameworks and governance.

It is intended to give this cohort confidence in overseeing cyber risk frameworks and programs, in asking the right questions, and in evaluating the information provided to them.

While organisations vary greatly in size, risk maturity levels, governance structures and regulatory obligations, this guide is intended to provide an overview of the governance and risk issues they should consider.

Senior management teams that oversee technology, product and other systems and process changes, should also understand the cyber risk practices within the organisation's overall risk management framework and ensure they are implemented within their areas of remit.

For those involved in implementing cyber risk frameworks, this Guide provides a holistic view encompassing governance, risk management, cybersecurity and standards.

---

1 Article *ASIC to target boards, execs for cyber failures*, Australian Financial Review 19 September 2023 and *Interim Policy and Supervision Priorities Update*, Letter to All APRA-regulated entities, 31 January 2024.

2 *The Global Risks Report 2024,* 19th Edition, World Economic Forum.

3 https://www.weforum.org/agenda/2023/06/asia-pacific-region-the-new-ground-zero-cybercrime/#:~:text=The%20average%20annual%20cost%20of,compared%20to%20its%20global%20counterparts.

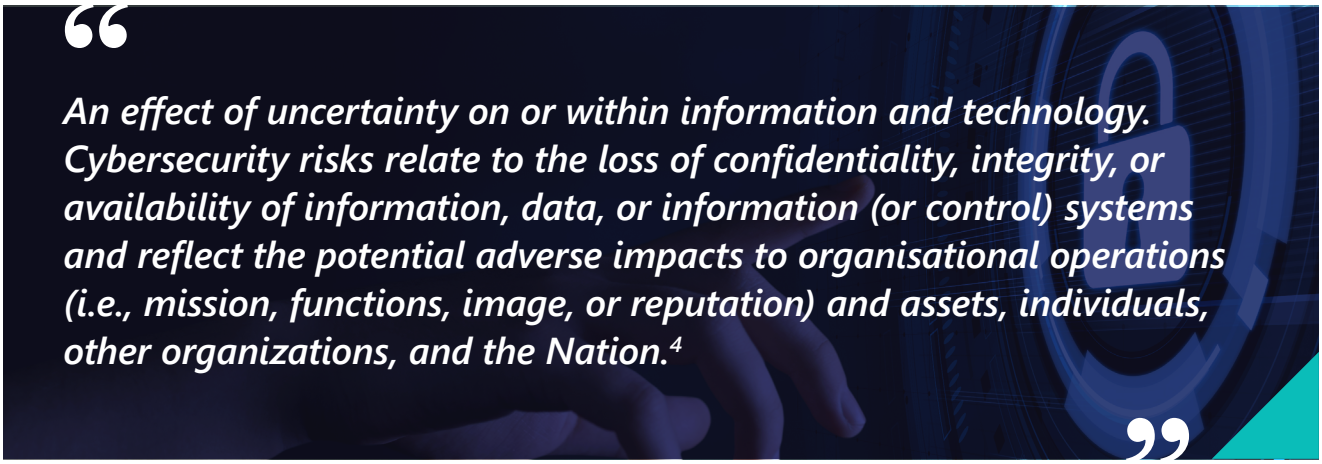
Navigating this guide

Reader type	Some question I'm currently thinking about	Jump to
Beginner	I'm new to cyber risk management and need to know where to start. I have yet to implement a cyber risk management strategy. I have a small team and require useful implementation tools. I have limited knowledge of organisational cyber risks.	Chapter 4 – What is Cyber risk? Chapter 6 – Elements of a Cyber Risk Management Framework
Intermediate	I want to improve on my existing cyber risk systems. I have operationalised some cyber security frameworks but nervous they are not sufficient. I report to a Board of Directors and have primary operational responsibility. I have some knowledge of organisational cyber risk and how to manage it.	Chapter 5 - Key elements of governance Chapter 6 - Elements of a Cyber Risk Management framework Standards, Frameworks and Certifications
Advanced	I have developed cyber risk management strategies. I want to understand how to integrate cyber risk into the organisation's strategic risk framework. I want best practice strategies to improve on my current cyber risk systems. I need a better understanding of the regulatory landscape.	Chapter 6 - Elements of a Cyber Risk Management framework Chapter 7 - Risk Management Process Chapter 9 - The Regulatory landscape Chapter 11 - International regulations

4. What is Cyber Risk?

One of the potential barriers for directors, executives, governance professionals, and some enterprise risk professionals in assessing cyber risks, is the technical language used to describe cyber risks and threats. This can be challenging for those with a non-technical background. This section provides some definitions and examples to empower you with the knowledge to initiate and lead conversations.

The National Institute of Standards and Technology (NIST), a non-regulatory agency of the U.S. Department of Commerce, and a leading global authority on the development of cyber risk management frameworks, defines cyber risk as,



A Cyber Risk Matrix can illustrate the potential scope of cyber risks and associated cyber risk categories. A non-exhaustive list of cyber risk categories is provided.

Cyber Risk type	Financial	Legal	Operational	Reputational
Threat of extortion				
System and service disruption and outages				
Loss of productivity				
Theft of sensitive commercial data, IP or trade secrets				
Customer data theft				
Regulatory non-compliance				
Loss of consumer trust and customer attrition				
Public relations and media backlash				

Is 'cyber security' the same as 'information security'?

The terms may be used interchangeably, however there is an important distinction. Cyber security is broader and may encompass security risks beyond information to include communication and other network systems and activities. NIST provides the following useful definitions:

Information security – 'The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability'.[5] This is also the definition adopted by the Australian Cyber Security Centre (ACSC).[6]

4 See Glossary, Computer Security Resource Center, National Institute of Standards and Technology (NIST).

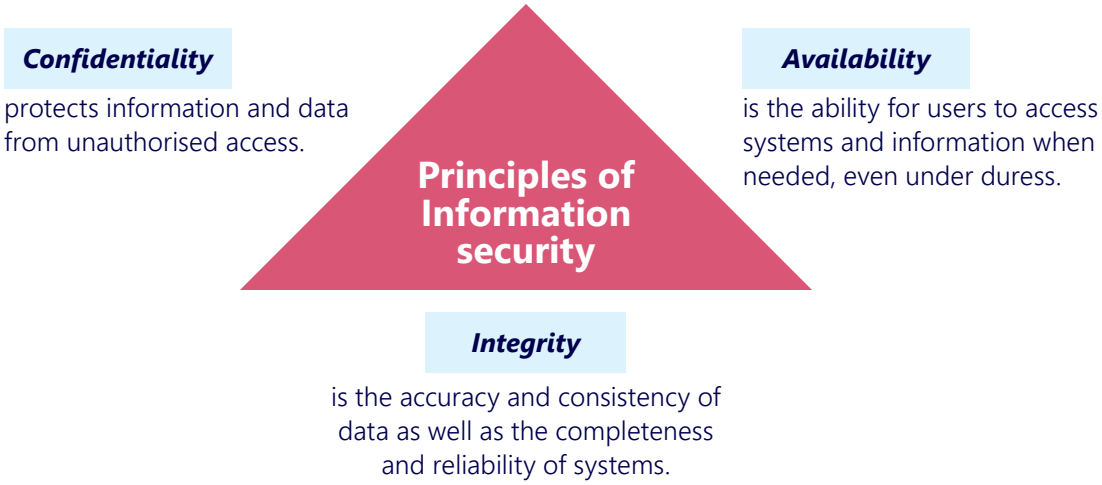
5 See NIST Glossary

6 See Glossary, Australian Cyber Secirity Centre (ACSC)

Cybersecurity – 'The ability to protect or defend the use of cyberspace from cyber attacks', with cyberspace being 'the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers'.[7]

What to consider when identifying information and cyber risks

The three principles of information security are illustrated below, as confidentiality, availability and integrity.



Cyber risks on the other hand are much broader and can relate to data security, on premises systems, the cloud, third party supply chain, human risks, compliance risks and technical risks. It covers both 'insider' threats from employees or partners that may not be intentional, and 'external threats' from malicious actors and cyber criminals. The table below includes some cyber risk examples.

7 See NIST Glossary

Examples of cyber threats

Business Email Compromise

Email fraud targeting business, government and non-profit organisations to achieve a specific outcome which negatively impacts the target organisation.[8]

An example of business email compromise is email spoofing, which is a type of cyberattack that targets businesses by using emails with forged sender addresses. Because the recipient trusts the alleged sender, they are more likely to open the email and interact with its contents, such as a malicious link or attachment.[9]

Data breach and data exfiltration

A data breach is the unauthorised movement or disclosure of sensitive private or business information.[10] A data breach occurs when sensitive or personal information is accessed, disclosed or exposed to unauthorised people. This can occur accidentally or as the result of a security breach.[11]

Data exfiltration typically involves a cybercriminal stealing data from personal or corporate devices, such as computers and mobile phones, using various cyberattack methods. A common data exfiltration definition is the theft or unauthorised removal or movement of any data from a device.

Denial of service attacks and Distributed Denial of service attacks

Denial-of-service (DoS) attacks are designed to disrupt or degrade online services such as websites, email, and Domain Name System (DNS) services. To achieve this, malicious actors may use a number of approaches to deny access to legitimate users of online services such as:

- using multiple computers to direct a large volume of unwanted network traffic at online services to consume all available network bandwidth
- using multiple computers to direct tailored traffic at online services in an attempt to consume the processing resources of online services, or
- hijacking online services in an attempt to redirect legitimate users away from those services to other services.[12]

A distributed denial-of-service (DDoS) attack is where the source is comprised of multiple, distributed unique IP addresses used to flood the bandwidth or resources of a targeted system or network.[13]

8 Glossary at cyber.gov.au.

9 *Email spoofing, How to identify a Spoofed Email*, crowdstrike.com.

10 Glossary at cyber.gov.au.

11 See Data breaches at cyber.gov.au.

12 See *Preparing for and responding to denial of service attacks*, ASD/ACSC.

13 Glossary at cyber.gov.au.

Examples of cyber threats

Malware

Malicious software, known as 'Malware', refers to any type of code or program used for a malicious purpose.

Cybercriminals use malware for many different reasons. Malware is commonly used for:

- stealing information and account details
- encrypting data for ransom, or
- installing software without the user's knowledge.

A malware attack can have serious and ongoing impacts. Malware can also act as an entry point for cybercriminals, opening the door to further malicious activity.

Malware can be distributed in several ways:

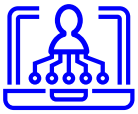
- by spam email or messages, either as a link or an attachment
- by malicious websites that attempt to install malware when users visit
- by exploiting weaknesses in software on devices such as laptops and mobile telephones
- by posing as a trusted application that users download and install themselves, or
- Pretending to be antivirus or security products.[14]

Man-in-the-middle-attacks

A man in the middle (MITM) attack occurs when cybercriminals intercept and alter network traffic flowing between IT systems. The MITM attack impersonates both senders and receivers on the network. It aims to trick both into sending unencrypted data that the attacker intercepts and can use for further attacks or financial gain.[15]

Phishing attacks

Phishing is how cyber criminals trick individuals into providing personal information. They send fraudulent emails or text messages often pretending to be from large, known, and trusted organisations. They may try to steal online banking logins, credit card details or passwords. Phishing can result in the loss of information, money, or identity theft. For example, spear-phishing is when these emails and text messages are highly targeted to a recipient.[16]



Ransomware

Ransomware is a common malware that makes data or systems unusable until the victim makes a payment.[17] It works by locking up or encrypting files so they can no longer be accessed. A ransom, usually in the form of cryptocurrency, is demanded to restore access to the files. Cybercriminals may also demand a ransom to prevent data and intellectual property from being leaked or sold online.

Ransomware as a service (RaaS) is a malicious adaptation of the software as a service (SaaS) business model. It is a subscription-based model that sells or rents predeveloped ransomware tools to buyers, called ransomware affiliates, to execute ransomware attacks.[18]

14 See 'Malware' at Cyber.gov.au.

15 See *Types of Cybersecurity attacks* at Rapid7.com.

16 *Phishing Learn about phishing attacks and know what to do if you've been targeted*, at cyber.gov.au.

17 Glossary at cyber.gov.au.

18 *What is Ransomware as a Service (RaaS)?* at paloaltonetworks.com.au.

5. Key elements of governance

The cyber governance process should be encompassed within the overall corporate governance framework of the organisation, and should be appropriate to that organisation's type, ownership structure, size, industry, and risk profile.

The role of the board and board committees

The board is responsible for overseeing the corporate governance of an organisation and managing risk. It is also responsible for the organisation's performance and for overseeing the management of a range of internal and external stakeholders, including shareholders, but also, in the context of cyber risks, customers, individuals and often, the public.

Directors' duties

Australian company directors have general fiduciary duties under both statute law and common law to act with care and diligence. Boards of APRA-regulated entities are 'ultimately responsible for the information security of an entity'.[19] There are increasing regulatory expectations in relation to directors' responsibilities for cyber risk. For example, in an action by ASIC, the board of an entity holding an Australian Financial Services Licence was held to be in breach of the *Corporations Act* for failing to manage cyber risks.[20] The Australian Information Commissioner has also recently brought civil penalty proceedings against Medibank Private Limited in relation to its October 2022 data breach alleging that Medibank seriously interfered with the privacy of 9.7M individuals by failing to take reasonable steps to protect their personal information from misuse and unauthorised access and disclosure in breach of the Privacy Act 1988.[21]

> *The board's role is to understand the threat environment, set the risk appetite, ensure adequate resources are allocated to the task, and then (either directly or through a sub-committee) monitor and oversee the development, maintenance, and implementation of suitable systems and processes for cyber defence, incident response and recovery, and cyber resilience.*[22]
>
> ***At the same time, directors can harness the benefits that technology offers to an organisation.***

19 See APRA *Prudential Standard CPS 234 Information Security*.

20 *ASIC vs RI Advice Group Pty Ltd [2022]* FCA 496.

21 See *Corporate governance implications of Medibank enforcement proceedings*, John Keeves, June 2024.

22 See Cybersecurity governance: are directors doing enough?, Professor Pamela Hanrahan, March 2024.

The role of the board

The board plays an important role in risk management. General knowledge of cyber security is fundamental in the development and authorisation of strategy and decisions. The table below provides questions and activities that the Board may want to consider.

Board checklist

- ☐ Are processes in place to monitor the evolving regulatory landscape and is the Board sufficiently informed about current and prospective laws and standards ahead of meetings and when decisions are being made?
- ☐ Is the organisation's risk framework regularly reviewed and does the board have processes to ensure management obtains independent advice and assurance where required?
- ☐ How does the Board ensure a whole-of-organisation risk culture, including a security-aware culture?
- ☐ Ensuring the appropriate and balanced level of investment in cyber security relative to the cyber risks facing the organisation.
- ☐ Deciding on the appropriate cyber governance structure to meet business goals.
- ☐ Ensuring the board receives appropriate education on cyber security and risk management.
- ☐ Overseeing the overall governance framework, including risk management and cyber security.
- ☐ Ensuring appropriate reporting to the board, or through its committees, on cyber strategies, risks, projects, and activities,
- ☐ Requiring management of stakeholders, including shareholders, customers, regulators, and the community.
- ☐ Ensuring that contracting risk is managed in accordance with the organisation's delegations framework.
- ☐ Understanding and overseeing data governance.

A challenge for boards is acquiring and developing relevant knowledge and skills in cyber risk, so that they can confidently and effectively oversee cyber risk programs and challenge management as required. Boards can consider including cyber risk management in its 'skills matrix' to ensure there are relevant skills at board and/or board committee level.

A further challenge for boards is defining cyber risk materiality and setting measurable risk appetites and tolerances in relation to cyber risks. This drives investment in cyber security capabilities and systems and informs performance targets and goals.

Board committees

Depending on the organisation's committee structure, it can be appropriate to include cyber risk management within the remit of a board-level Risk Committee, Audit Committee, Technology Committee, or a standalone Cyber Committee. This is of particular relevance for larger boards and organisations with detailed and complex cyber risks. Smaller organisations may decide to hold all discussions at board level.

Where there may be gaps in internal capability, knowledge, and experience, it may be appropriate to augment a committee with external members to provide more skills related to specific gaps such as data governance, threat protection or identity protection.

ASIC'S key questions for boards of directors

Risk management framework

- ☐ Are cyber risks an integral part of the organisation's risk management framework?
- ☐ How often is the cyber resilience program reviewed at the board level?
- ☐ What risk is posed by cyber threats to the organisation's business?
- ☐ Does the board need further expertise to understand the risk?

Monitoring cyber risk

- ☐ How can cyber risk be monitored and what escalation triggers should be adopted?

Controls

- ☐ What is the people strategy around cyber security?
- ☐ What is in place to protect critical information assets?

Response

- ☐ What needs to occur in the event of a breach?[23]

Accountability and responsibility

An important component of governance is ensuring that accountabilities and responsibilities for cyber risk management are well defined and that everyone in the organisation is aware of them.

How responsibilities are allocated will vary widely between different types of organisations, depending on their industry, size, risks, regulations, and level of resourcing. Some organisations may have a dedicated Chief Information Security Officer. In other organisations, responsibility for cyber risk may fall under the remit of the General Counsel, Chief Technology Officer, Chief Risk Officer, or Chief Financial Officer. In smaller organisations, management accountability may rest with the Chief Executive Officer, with the detailed tasks being outsourced to an external provider.

Given that responsibility may be dispersed across many individuals and committees, coordination of cyber risk management efforts is crucial.

For APRA regulated entities, defining roles and responsibilities for information security is required under APRA Prudential Standard CPS 234 Information Security. This includes clearly 'defining the information security-related roles and responsibilities of the Board, senior management, governing bodies and individuals with responsibility for decision-making, approval, oversight, operations and information security functions'.[24] However, defining roles and responsibilities is good governance practice for all organisations.

Reporting

Reporting to both boards and management teams is an important area that typically evolves as organisations' cyber risk maturity increases.

It is useful for decision-makers, whether directors or management, to agree on the information and metrics required to oversee cyber risk. This may include risk appetite and tolerance levels, where they have been established. It is also useful for the board and executives to receive reports and information that will contextualise the metrics. For example, educational updates on cyber risk trends on the organisation's key assets, or an overview of technology architecture.

23 See *Key questions for an organisation's board of directors*, ASIC.

24 APRA *Prudential Standard CPS 234 Information Security*, section 14.

It may be appropriate to consider using a cyber risk dashboard to provide a high-level overview of cyber risks, defences, projects and activities, with further detail available through supporting interactive or static reports.

Some organisations may also wish to consider how they can develop cascading risk registers where detailed operational cyber risks 'feed up', into higher-level cyber risks, and in turn, into the enterprise risk register. The same approach could also be used for cascading cyber operational plans, programs, and corporate strategic initiatives.

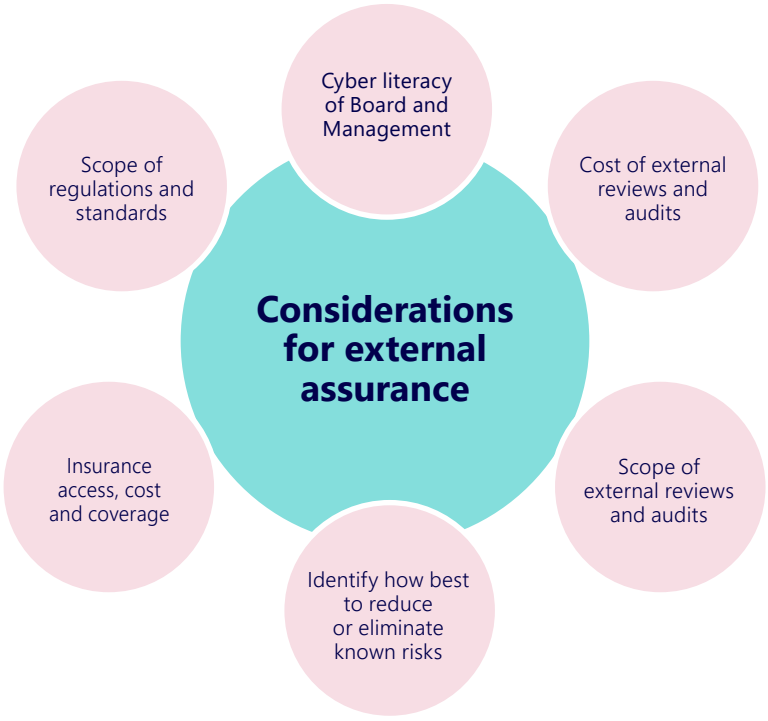
Questions to consider for cyber risk reporting

- ☐ How often should the board and executive team receive reporting on cyber risk?
- ☐ How often should the board discuss cyber risk with management?
- ☐ How are cyber risk appetite or tolerance levels defined and measured to inform reporting levels?
- ☐ What are the most useful cybersecurity metrics to report to boards and executive teams in your organisation?
- ☐ What other reporting or information do they need to put these metrics in context? (For example, an overview of technology architecture).
- ☐ How can we ensure the information is both accurate and timely?
- ☐ How much information is too much or not enough?
- ☐ What constitutes an incident disclosable/reportable externally? Have we checked the current legislative requirements relevant to our industry and organisation?
- ☐ How does the board determine materiality in relation to cyber security risks to inform prioritisation and compliance with disclosure requirements?

Assurance

A challenge for boards and management is obtaining reliable assurance that the organisation is effectively protected from cyber risks. Some organisations have an internal audit or assurance function, which may play a role in cyber risk and controls assurance.

The extent to which external assurance is required will depend on the following factors:



- Scope - boards should consider what is covered in the scope of external reviews and audits, and importantly, what is excluded. For example, an external financial audit by the organisation's auditor may include testing of information technology controls, but only those that relate to the production of financial reporting.
- What regulations and standards, if any, apply to the organisation? What is the scope of these regulations and standards, and conversely, what is not covered by those regulations and standards?[25]
  Board and management cyber knowledge and expertise in reviewing cyber risk management reporting.
- The costs of external audits and certifications.
- Insurance access, costs and coverage.

When engaging external providers, there is a need to obtain assurance in relation to their cyber security management practices. These obligations can be included in contracts with suppliers; however, that may not be possible when a smaller organisation is using a larger provider and has limited contractual bargaining power. Ultimately, boards and management teams should consider whether it is appropriate to continue to use the systems and services of third-party providers who are unable or unwilling to provide comprehensive information about their cybersecurity systems and practices.

Organisations should also consider whether they have assumed contractual requirements to adhere to specific standards or certifications or undergo periodic audits. These audits may also be useful for boards and internal management to provide a level of assurance that appropriate processes and controls are in place and identify any gaps in controls and practices.

25 Note that industry best practice and International Standards Organisation (ISO), ISO /ASA /BSI standards, such as *ISO 27000 Information security, cyber security and privacy protection* have a compliance aspect where businesses can be certified as compliant. Some other best practice guidance frameworks are intended as an operational guide only.

6. Elements of a Cyber Risk Management Framework

Start with a cyber risk strategy

Ideally organisations need to develop a cyber risk strategy, overseen by the board, that is appropriate to their size and scale. A cyber risk strategy appropriately assesses the current cybersecurity and compliance posture, identifies how best to reduce or eliminate known risks, and manages future risk exposure through systems and processes that monitor, evaluate and adapt current approaches.[26] [27]

Assess current cybersecurity and compliance posture

1. Conduct a thorough risk assessment by identifying valuable assets and evaluating critical vulnerabilities
2. Develop of a Cyber Risk Management Framework
3. Communicate key issues up to the board

Identify how best to reduce or eliminate known risks

1. Quantify the risk by identifying probability and avoidance costs
2. Develop a risk appetite framework
3. Develop benchmarks to manage the risk environment
4. Consider the cost of each approach based on the
5. Assess cyber literacy
6. Consider adopting a standard
7. Seek independent third-party advice and support

Manage future risk exposure and incident response

1. Integrate real-time threat detection systems
2. Have immediate response plans
3. Develop a Business Continuity Plan and implement preventative measures such as automated patch management systems
4. Cyber security awareness, education and training
5. Encourage security culture
6. Keep up to date with the latest information from ACSC and official news and regulatory and compliance changes

Monitor, evaluate and adapt

Organisations need to consider their overarching cyber security framework in light of a variety of guidance, standards, contractual obligations, and legislation.[28] At a high level, it is important to consider whether cyber security risk management is:

- integrated with the organisation's enterprise risk management framework
- compliant with all relevant regulatory requirements
- adhering to a cyber security standard adopted by the organisation
- embedded across the organisation through a cyber-aware culture, and
- adequately resourced with appropriate expertise.

The following section outlines these elements in detail.

26 https://www.ibm.com/security/digital-assets/strategy-risk-managementebook/pdfs/Strategy_Risk_Management_EB.pdf

27 https://www.steadfastsolutions.com.au/insights/5-cyber-security-risk-management-strategies/

28 See *Good Governance Guide Cyber Security*, Governance Institute of Australia.

Integration with Risk Framework

An issue to consider is whether to integrate cyber risk management into the organisation's Risk Management Framework at an enterprise level as part of a 'whole of organisation' approach to risk management.

At a more granular level, it may not always be practical, as there is a need for cybersecurity standard processes, procedures and tools. At this level, cyber frameworks are usually more detailed, technical and prescriptive. This level of detail does not typically appear in the enterprise-wide framework but should be consistent with it.

Section 5 of this guide describes the risk management process itself, however cyber risk will also be inherent in other processes, such as data management and data governance, crisis management, business continuity and disaster recovery.

Organisations in some sectors (see Section 8) may be subject to specific requirements in relation to their risk frameworks. For example, APRA-regulated entities need to be aware that APRA continues to include a 'heightened supervisory focus on cyber resilience' as one of its priorities, with the objective that 'all regulated entities must ensure they take steps to be resilient against the growing threat of cyber-attacks'.[29]

The Protective Security Policy Framework (PSPF) and the Information Security Manual (ISM) will generally be relevant for Australian public service agencies and organisations providing information and communication technology (ICT) services to government.

Adopting a Standard

In addition to complying with any legislative requirements relating to cyber risk management and information security, organisations can also adopt voluntary standards, some of which also offer certification.

It is important for organisations to consider the benefits and costs of implementing the risk management frameworks and controls aligned to the standards below. The benefits include assurance of a strong cyber security posture for internal stakeholders, such as boards and management, and demonstrating a commitment to strong cyber security for external stakeholders including shareholders and investors, customers, suppliers and regulators.

An increasing number of business customers, both private and government, require adherence to a cyber security, risk management or information technology standard as a contractual requirement.

However, implementing programs and controls and external audits and certifications can also have significant costs, which will also factor into an organisation's decision.

Below are commonly used standards and frameworks.

1. Essential 8

The Australian Cyber Security Centre (ACSC) developed the' Essential 8' as a baseline that organisations can adopt as a first step. Organisations can measure their maturity levels against the Essential 8 model. ACSC recommends that organisations aim for the same maturity level across the eight mitigation strategies.

The 8 mitigation strategies constituting the Essential 8 are:

- patching applications
- patching operating systems
- implementing multi-factor authentication
- restricting administrative privileges
- application control
- restricting use of Microsoft Office macros
- user application hardening, and
- regular backups.[30]

29 See *Interim Policy and Supervision Priorities Update*, APRA, 31 January 2024.

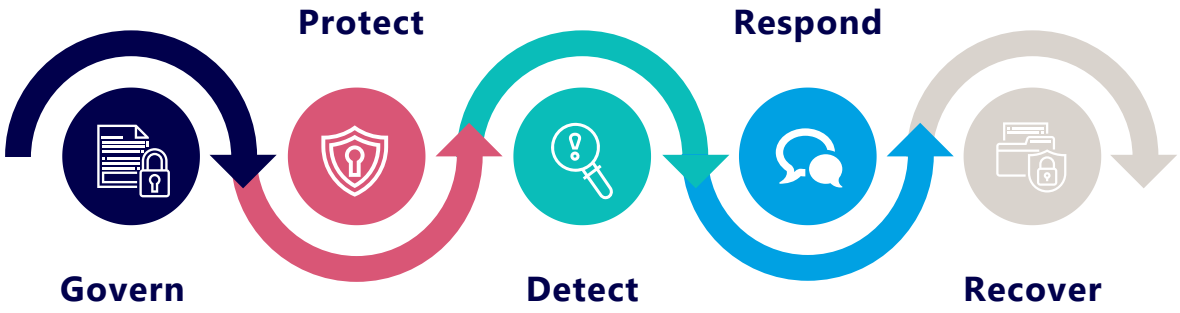
30 See Essential 8 explained at cyber.gov.au.

Source: Australian Cyber Security Centre

2. Information Security Manual (ISM)

The ISM was also developed by the ACSC with advice from the Australian Signals Directorate (ASD). It is aimed at larger organisations with cyber security teams and established roles such as Chief Information Security Officers and Chief Information Officers. It outlines a cyber security framework that takes a risk-based approach and can be applied using an organisation's existing risk management framework.

The manual outlines five 'cyber security principles'[31]



It also provides guidelines for

Cyber security roles	Cyber security incidents	Procurement and outsourcing
Security documentation	**Physical security**	**Communications infrastructure**
Communications systems	**Enterprise mobility**	**Evaluated products**
ICT equipment	**System management**	**System monitoring**
Database systems	**Email**	**Networking**
Cryptography	**Gateways**	**Data transfers**

31 See information Security Manual, *Cyber Security Principles* at cyber.gov.au

3. NIST Cyber Security Framework

The National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) is a commonly used cyber security framework globally. Version 2.0 was released in February 2024.

The NIST framework is a set of guidelines designed to help organisations manage and reduce cybersecurity risks. The Framework provides a flexible approach for assisting organisations of all sizes, in any sector, to apply the principles and best practices of risk management to improving the security and resilience of their critical infrastructure.

The NIST Framework consists of three main components:

Component	Description
Core	A set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. It is organised into five functions: Identify, Protect, Detect, Respond, Recover.
Tiers	Tiers describe the degree to which an organisation's cybersecurity risk management practices exhibit the characteristics defined in the framework (from Partial to Adaptive).
Profiles	Profiles are used to identify opportunities for improving cybersecurity posture by comparing a 'Current' profile (the 'as is' state) with a 'Target' profile (the 'to be' state).

It is important to note that the Framework is voluntary and serves as a guide rather than a set of mandatory regulations. Organisations can use the Framework to determine their current level of cybersecurity, set goals for cybersecurity measures, and establish a plan for improving or maintaining their cybersecurity posture.

Steps for creating and using a Cyber Security Framework: Organisational profile

Source: NIST Framework 2.0.

Source: NIST Framework 2.0.

4. ISO 27001:2022 Information security, cybersecurity and privacy protection Information security management systems - Requirements (ISO 27001: 2022)

ISO 27001:2022 developed by the International Standards Organisation (ISO) is an international standard against which it is also possible to obtain certification. It is the world's best-known standard for information security management systems (ISMS) and defines requirements that ISMS must meet but is broader than cyber.[32] It provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system.

ISO 27001 promotes a holistic approach to information security: vetting people, policies and technology. An information security management system implemented according to the Standard is a tool for risk management, cyber-resilience and operational excellence.

Organisations or businesses that conform to ISO 27001 have put in place a system to manage risks related to the security of data it owns or handles, with that system respecting all the best practices and principles enshrined in the Standard.

32 *See ISO 27001:2022 Information security, cybersecurity and privacy protection Information security management systems - Requirements (ISO 27001: 2022)*, International Organization for Standardization, Edition 3 2022.

Given the increasing levels of cybercrime and new threats constantly emerging, it can seem difficult or even impossible to manage cyber-risks. ISO 27001 is intended to help organisations become risk-aware and proactively identify and address weaknesses.[33]

5. Other useful standards

Other useful standards in commercial use include Microsoft secure score and Center for Internet Security Controls (CIS) critical security controls.[34]

Refer to Section 8 for a reference list of standards, frameworks and certifications.

Role of Culture

Creating a cyber-aware culture is essential to managing cyber risk. Risk management in general, including cyber risk, is not only about systems and hardware, but about people. People at all levels of an organisation can make decisions that have adverse impacts, be manipulated through social engineering and make mistakes. They can also be proactive and vigilant, protecting the organisation.

A cyber-aware and cyber-resilient culture will only be effective if it is within an overall culture of transparency and 'speaking up', which promotes good governance and risk management generally. This will make it easier and more likely that people will speak up and raise cyber risks.

A critical element of a cybersecurity framework is regular training, awareness and incident exercises. A cyber-aware culture will also encourage people to report suspicious activities and incidents, for example, phishing emails or texts, and integrate consideration of cyber risk into their decision-making. This may occur at the board or executive level but should also be part of other forums and committees making decisions about systems changes, new products or processes.

During technology transformations, or any IT projects, it may be appropriate to conduct a cyber impact assessment. This assessment considers how the new project may impact the cyber posture of the organisation, including its attack surface. It answers questions such as:

- Will this project introduce any new cyber risks, such as a third-party backup system?
- Will this project create, remove, amplify, or diminish any cyber controls?
- Where will data be stored?
- Who should have access to the systems and data in the new project?
- To what extent is artificial intelligence used in the new applications and does this give rise to any new threats?
- How will the existing cyber risk management framework and data governance framework be affected by the new project?
- Will any new personal or sensitive information be stored and how will this be managed?
- Will the new system require any additional data classifications or labels?

Capability and resourcing

Regardless of the strength of an organisation's cyber security framework, it will not be effective without the skills, expertise, and resourcing to implement it. This includes attracting the right talent either internally or externally and ongoing training for both frontline employees and management.

There is also an increased need for technical professionals to understand business strategy, objectives, and processes, and to effectively communicate in business terms. This should be considered when recruiting or outsourcing these roles.

A 'whole of organisation' approach to cyber risk management needs to consider how a potentially broad group of individuals or teams will work together. Effective cyber risk management will require skills in cybersecurity, information technology generally, risk management, legal, communication and other skills. It will often include both internal and outsourced teams.

Key to achieving this approach is identifying the skills required to establish, implement, and maintain cyber risk practices, and clearly defining roles, expectations, and ways of working.

For smaller organisations, managing an outsourced provider may fall to one function. At the other end of the spectrum, larger organisations will have large teams that need to keep up to date with emerging technologies and evolving risks.

33 See Foonote 30 above.

34 See Microsoft Secure Score and Center for Internet for Security Controls.

Questions to ask about your framework

Risk Assessment

- ☐ How are cyber risk assessments incorporated into our risk framework and processes?
- ☐ Is there a process for quantifying risks?

Preparedness

- ☐ How have we prepared for known / plausible information security risks?
- ☐ Has the organisation undertaken an exercise to understand its information assets and the threats and vulnerabilities relating to those assets?
- ☐ Has a control assurance program been established to confirm the above?

Information security

- ☐ Who has been given responsibility for managing information security and who is ultimately accountable?
- ☐ Have effectively designed and operating controls been implemented to prevent, detect and respond to information security incidents?
- ☐ Does the organisation have the necessary skills and capabilities (at all levels – including the board) to interpret and understand information security matters and make appropriate decisions?
- ☐ Have reporting and metrics and measurable risk appetites/thresholds/tolerances been established to enable information security oversight and decision making?

Costs

- ☐ How has control cost-effectiveness been determined to ensure the control cost is proportionate to the risk/risk reduction?

People and culture

- ☐ Have the organisation's employees been trained around potential threats to the organisation, and on their information security responsibilities?
- ☐ Have background checks or security clearances been used to establish trust in the organisation's employees?
- ☐ Do the organisation's policies, procedures and processes align with legal and regulatory requirements and/or best practice?
- ☐ Are staff encouraged to report suspicious activities and incidents?
- ☐ Are there organised drills to simulate a cyber-attack scenario?
- ☐ Is the responsibility for cyber security siloed in the organisation?

Cyber security

- ☐ How is the cyber risk appetite set by the board operationalised by the cyber security framework?
- ☐ How does the board determine materiality in relation to cyber security risks so as to inform prioritisation and possibly compliance with disclosure requirements?

Data

- ☐ Does our framework include risk assessment of third parties, including the risk of sharing information, or providing access, to third parties?
- ☐ Have we identified the organisation's critical assets?
- ☐ Do we have a process for data governance and protection?

7. Risk Management Process

There is a growing recognition of the importance of resilience to cyber-attacks, with ASIC noting that it is 'essential to all organisations operating in the digital economy'.[35]

Organisations that are cyber-resilient need to include cyber security as part of their overall risk management efforts. Incident management and response has become ever more important to boards, executives and the community following the COVID-19 pandemic and high-profile cyber-attack incidents in Australia.

Risk identification, assessment and evaluation

Understanding the organisation's cyber risk profile and vulnerabilities is essential to assessing the effectiveness of risk management, controls, standards and where priorities should lie.

To understand risks, organisations need to understand what is at risk – that is, what is of value to the organisation? This will vary between organisations. It may be a combination of data, reputation for seamless operations, physical assets and infrastructure, or revenue which is dependent on one asset, such as a website. Identifying and assessing risks requires understanding the context in which the organisation operates.

As technology evolves, so do cyber risks. Organisations need to consider reviewing their cyber risks and controls when introducing new technology, new suppliers or changing technology.

If the organisation already has a risk management process, it can be useful to use its existing risk management processes for the identification, assessment and recording of risks, for example, on a risk register.

Questions to ask about your cyber risk profile may include:

- ☐ Threat actors - are you likely to be a target of any of the following: cyber criminals seeking extortion or denial of service, state actors, hacktivists, competitors, disgruntled current employees, or ex-employees?
- ☐ Are you exposed to supply chain risks, including third and fourth parties in your ecosystem?
- ☐ Have you identified your internal skills and system vulnerabilities including an assessment of key processes, systems and people? And what policies are in place to manage these risks?
- ☐ Have you adopted new technologies such as cloud computing, the internet of things (IOT) or artificial intelligence (AI)?
- ☐ What data do you hold? How much data is too much data? Is organisational or customer data held by third parties? What are your 'crown jewels'?
- ☐ Human risks - What are the human risks, both internal and external?
- ☐ Shadow AI – How is management ensuring that AI used within the organisation is sanctioned, within policy and known to IT and the cyber team?

Based on the answers to the above:

- ☐ What risk/threat scenarios are most relevant to your organisation?
- ☐ What constitutes a material cyber risk or incident, and do we have appropriate controls in place for our material risks?
- ☐ What would cause harm and vulnerability to the organisation:
  - ☐ loss of other parties' data?
  - ☐ disclosure of confidential information?
  - ☐ inability to operate and serve customers or the public?
- ☐ What is the threshold for notifying executive management and the board of a cyber event?
- ☐ Do we have a security operations centre (SOC) in place and is it monitored 24x7x365?
- ☐ Do we use a threat intelligence feed in our cyber defences?
- ☐ Do we regularly assess the effectiveness of our cyber risk management systems?
- ☐ When did we last run a penetration test and vulnerability assessment?
- ☐ Have there been any recent breaches or near misses?

35 See *Cyber resilience* at asic.gov.au.

Risk treatment and controls

Risk treatment needs to consider controls for both technical and human risks, and consider external attack, as well as internal attack or error. The control framework should include preventative, detective and corrective controls. Risk treatment also includes mitigation and recovery.

It is not possible to list all possible controls. Many are outlined in the standards referenced in this publication and include:

- Security by design - that is, considering cyber risks early in the process of planning technical changes and product development, rather than conducting a review at the end and needing to accept risks or significantly change designs.
- Intelligence - understanding the threat environment.
- Taking a 'zero trust' approach to providing access to information and data only to roles that require it via Roles Based Access Controls (RBAC).
- Policies as part of the Cyber Security Program – for example, data classification, use of technology, asset management and maintenance.[36]
- Access controls to sensitive information, including revoking system and information access rights that a user no longer requires, for example, if someone changes roles and responsibilities or leaves the organisation.
- Some legislation may require background checks and clearances for employees and contractors.
- People controls – training, testing, for example, for social engineering.
- External testing - both of people and systems, for example, penetration testing.
- Detection controls - for example, an intrusion detection system detecting suspicious activity.[37]
- Mitigation through incident response plans, or through risk transfer, for example, insurance. See the section below for more details.
- How best to test controls and identify gaps. As outlined in Section 9, there are frameworks that can assist organisations with cyber security controls.

Incident, crisis management and business continuity planning

Incorporating cyber security incident planning to Crisis and Business Continuity Planning (BCP) frameworks

With an increased focus on organisational resilience, it is essential for organisations to incorporate cyber security events into their incident management, crisis management, IT disaster recovery and business continuity processes. These concepts are outlined in more detail below.

Business Continuity – the capability of an organisation to continue the delivery of products and services within acceptable timeframes at a predefined capacity during a disruption.[38]

Crisis management - response to a disruptive event, in an effective, timely manner, with the goal of avoiding or minimising damage to the organisation's profitability, reputation, and ability to operate.[39]

Incident – an event that can be, or could lead to, a disruption, loss, emergency or crisis.[40]

It is good practice for organisations to have crisis management plans and business continuity plans that can be used by executive teams, boards, and response teams in a range of situations. Such plans are broad enough to cover not only cyber security events but also situations such as natural disasters, pandemics, legal or reputational crises and system failures.

The challenge for organisations is to have a plan outlining key people, key roles and how the various teams will work together that is not too prescriptive to apply to unexpected events, and yet also includes a number of prescriptive response plans for specific scenarios.

36 ISO27001:2022 Annex A contains a list of 93 controls, grouped into four themes: organisational, people, physical and technological.

37 Intrusion detection systems (IDS) can be classified into two types: Signature-based IDS which use predefined signatures of known threats to detect intrusions, and Anomaly-based IDS which use machine learning to establish a baseline of normal behaviour and then flag any deviations as potential threats.

38 *ISO 22301: 2019 Security and Resilience – Business Continuity Management Systems – Requirements*.

39 *BCI/DRJ Glossary of Terms*, Business Continuity Institute.

40 *ISO 22301: 2019 Security and Resilience – Business Continuity Management Systems – Requirements*.

A risk-based approach to specific scenarios that are most likely to occur and would have the most impact if they did occur can be helpful. For example, a response plan for theft of sensitive data and mandatory data breach notification, ransomware or other extortion demands, or a denial-of-service system disruption. Ideally, these scenarios would be consistent with the cyber risks identified and assessed during the organisation's risk assessment process.

The international standard for business continuity management systems is *ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements*.[41] It provides a framework for organisations to plan, establish, implement, operate, monitor, review, maintain, and continually improve a documented management system to protect against, reduce the likelihood of, and ensure recovery from disruptive incidents.

The *Good Practice Guidelines* (GPG) is another guide for business continuity and resilience professionals. The GPG is used as an information source for individuals and organisations seeking an understanding of business continuity as part of their awareness-raising campaigns and training schedules. The GPG takes a collaborative approach to business continuity, ensuring organisations and individuals understand how to work with related management disciplines to fit in crisis planning.[42]

Planning

The business continuity planning stage involves identifying which systems and processes are critical, assessing the impact of a cyber event, and outlining how the organisation would continue to operate during the disruptive event and recover.

Incident management planning involves outlining what an incident, in this case, a cyber incident, could be and how the incident management team would identify there is an incident, classify the incident, contain or escalate it. Incident management plans typically include the classification of incidents, including where they have become crises.

The crisis management plan should define what constitutes a crisis for the organisation, outline the role of the crisis management team, and specify who is required in a cyber crisis. This may involve challenging questions and conversations about whether board members or particular senior executives should be actively involved because they would add value in the situation or should be informed. This will vary across organisations.

For cyber security incidents a Cyber Security Incident Response Plan (CSIRP) is often created which contains a number of 'playbooks' for effectively responding and recovering from an incident, and maintain services.

All plans need to outline roles and responsibilities for individual roles and teams, including boards, the executive, other leaders, internal and external communication, technology and legal. They should also outline how often the teams will meet and how they will record the issues and decisions.

Communication is vital at all points in the process. Cyber events can move rapidly and the larger the organisation is, the more people will be involved.

A key consideration is how the teams will interact, including the following:

- Crisis management (involving the senior executives and perhaps the board).
- Incident management teams and technical teams – isolating, backup restoration, forensics.
- Corporate teams managing legal and insurance.
- Customer management, and
- Media and public relations

It is helpful for organisational leaders to have considered potential decisions before a crisis event has occurred:

- Would the organisation pay a ransomware demand? Under what circumstances, for example, public safety. Would it be legal to do so, as it may not be legal in certain situations?
- What is the internal legal process, and should particular incidents be reported to law enforcement where it is not a legal requirement to do so?
- In a cyber event, who needs to be involved and who needs to be informed?
- What are the organisation's notification requirements – regulatory, contractually and reputationally?
- At what point should an insurer be notified, and if a claim is to be made, under which policy (noting, for example, that a claim for ransomware may be responded to by a cyber policy or a crimes policy)?

41 See https://www.iso.org/standard/75106.html.

42 See Good Practice Guidelines Edition 7.0, October 2023, The Business Continuity Institute.

The table below sets out the range of cyber incident notification requirements that apply in Australia.[43]

Cyber incident notification requirements	
Location	**Legislation/Standard**

All of Australia (depending on sector)	• APRA Prudential Standards:
	  o CPS 234 (Information security) – Notification of information security incident
	  o CPS 232 (Business continuity management) Notification of major disruption
	  o CPS 230 (Operational risk management) Notification of operational risk incidents.[44]
	• ASX Listing Rules – Continuous disclosure obligations[45]
	• Consumer Data Right – Notification of eligible data breach
	• My Health Records Act 2012 Notification of data breaches
	• Privacy Act 1988 – Notification of eligible data breach
	• Security of Critical Infrastructure Act 2018 – Notification of cyber security incidents in specific sectors
	• Telecommunications – Cyber security incident notification.

State based	• ACT - ACT Voluntary notification regime • NSW - Privacy and Personal Information Protection Act 1998 (NSW) - Notification of eligible data breach • NT - Northern Territory Voluntary notification regime • QLD - Queensland government enterprise architecture – Information security incident reporting • SA - Government of South Australia, premier and cabinet circular PC042 cyber security incident Reporting cyber security incidents • TAS - Tasmanian government incident management cybersecurity standard – Notification of cybersecurity events and incidents. • VIC - Victorian Protective Data Security Standards Information security incident notification • WA - Western Australian whole-of-government cyber security incident coordination framework Reporting cyber security incidents.

AUSTRAC has also issued guidance for data breaches in relation to AUSTRAC-regulated entities which are encouraged to notify AUSTRAC of data breaches.[46]

Training, tests, and exercises

Providing training to all those who have a role in incident or crisis management teams is key. Conducting regular exercises to validate the plan and document learnings and improvements is also important.

The frequency of exercises will depend on each organisation's circumstances, risk profile and process maturity. For example, an exercise involving the senior executives and the board may be conducted once a year, potentially including an external expert. However, incident teams that regularly respond to cyber incidents may choose to engage in exercises more frequently, for example, quarterly.

Exercise formats can range from desktop walkthroughs of the plans, guided facilitation or to 'surprise' exercises, depending on the maturity of the plans and the participants' experience.

43 For further detail on cyber incident reporting obligations see *Cyber Incident Notification Regulations in Australia 2023*, PwC, September 2023.

44 *CPS 230 Operational Risk Management* will apply from 1 July 2025. See article *CPS 230 Your roadmap to compliance*, Minter Ellison, 23 February 2024.

45 ASX has recently updated its Guidance Note 8 Continuous Disclosure to include a new data breach example. See *Listed@ASX Compliance Update no 6/24*.

46 See *Data breaches and AML/CTF considerations*, AUSTRAC, 19 January 2024.

Post-incident review and lessons learned

It is good practice to conduct a post-incident review of crises, incidents and near misses (incidents that occurred without harm or damage occurring) to review how the plans worked in practice and determine improvements for the future.

Emerging regulation and government assistance

Organisations should monitor emerging regulatory developments, particularly about privacy and data protection legislation and security of critical infrastructure and which include obligations and potential assistance on cyber incidents and ransomware. Refer to section 8 for further details.

Further regulatory changes may also arise from Australia's 2023 - 2030 Cyber Security Strategy as it is progressively implemented.[47]

Additional questions to consider

- ☐ Is it clear when a cyber security event will trigger the Crisis Plan?
- ☐ Is there an escalation procedure and criteria in your incident, business continuity and crisis plan that includes cyber events?
- ☐ Who makes key decisions? For example, declaring a crisis, contacting law enforcement, public announcements or paying ransom demands.
- ☐ What is the board's role in a cyber incident?
- ☐ Who should communicate with the media and other key stakeholders during a cyber event?
- ☐ Has the crisis plan been exercised/tested in relation to a cyber event scenario?
- ☐ Is government assistance available?
- ☐ Should an external provider, Security Operation Centre (SOC) / Cyber Incident Response Service, be engaged on retainer 24/7 to augment the central team?
- ☐ Are there contractual obligations regarding notification (for example, to business partners, customers, or suppliers?

Cyber insurance

Insurance is seen as a form of 'risk transfer', with the risk of financial costs of a cyber incident being assumed by insurers. It is not possible to insure against reputational damage and it is important to implement risk management and controls in addition to purchasing any insurance.

Further, the insurance market and increasing premium costs have played a large role in decision-making in recent years about whether to acquire a cyber insurance policy. Identifying and assessing the impacts of cyber risks in detail as outlined in this guide can help organisations make an informed decision on cyber insurance.

Standalone cyber insurance policies vary in terms of what they cover. In general, they cover 'first party costs', which are costs that are directly incurred by the insured party, for example, hiring forensic investigators. Policies typically also cover 'third party costs', which are costs for which an organisation could be liable to other parties because of the event. These could include compensation to customers, or fines issued by regulators, to the extent that such fines can be recoverable under insurance by law.

Specific areas of cover may include multimedia liability, security and privacy liability, privacy regulatory defence and penalties, privacy breach response costs, customer notification expenses and customer support and credit monitoring expenses, network asset protection, cyber extortion, cyber terrorism, Payment Card Industry Data Security Standard (PCI DSS) fines and assessments, and cybercrime, including financial fraud, telecommunications fraud and phishing attacks.[48]

47 See *Australia's Cyber Security Strategy 2023 – 2030*.

48 See *Cyber Insurance: Protecting our way of life in a digital world*, Insurance Council of Australia, March 2022.

Cyber cover may also be included in other insurance policies, such as indemnity policies; however, it is often specifically excluded from those policies. It is important to work with insurance brokers and insurers to understand where gaps in insurance coverage may exist, and where coverage may overlap.

The level of cover would ideally be aligned with the risk impacts and consequences calculated and assessed through the organisation's risk management process. This will also assist in seeking cyber insurance as insurers now require detailed information from organisations about their cyber risks and cyber security controls.

It is also important to note the role of cyber insurance in a crisis response to a cyber incident event. The professional advisors that may be accessed under cyber insurance policies, such as forensic, legal, and public relations advisors could be particularly useful for organisations that do not have internal capabilities. Organisations should investigate with their broker and insurer how this assistance would work in practice during a cyber event.

Cyber insurance tips

- Consider whether it is more cost-effective to purchase cyber insurance or self-insure.
- Consider engaging in cyber risk quantification to inform discussions on cyber insurance premiums and coverage.
- Ensure you are aware of the coverage provided in your specific policies. Coverage varies widely between the insurance policies available on the market, and this may not be apparent until a claim is made.
- Be aware of potential regulatory changes as this is a fast-moving area.
- Ensure any steps required during a cyber incident, such as notifying the insurer before expenses are incurred, are included in your organisation's incident management plan as well as their contact details if the insurer's external advisers will be used during an incident.
- Note that it can take time to assess the full financial impact of a cyber incident, which may impact the timeframe for receiving payment for an insurance claim.

8. The Regulatory Landscape

There is a broad range of regulations relating to information and cyber security relevant to Australian organisations. The following table contains a summary of some of the key legislative and other requirements but is not intended to be exhaustive. The cyber incident notification requirements referred to in Section 7 above will also be relevant.

Australian Privacy Principles **(APP)** **Regulator:** Office of the Australian Information Commissioner (OAIC) **Regulation**: *Privacy Act 1988*	The Privacy Act 1988 relates to how organisations collect, manage and dispose of personal information. Two key points to note in relation to the Act are: Australian Privacy Principle 11 – Security of Personal Information (APP 11) – requiring organisations to take active measures to ensure the security of personal information they hold and the **Notifiable Data Breaches (NDB) regime** which requires organisations to notify affected individuals and the OAIC as soon as practicable of a material data breach. Entities covered by the regime include Australian Government agencies and private sector and not-for-profit organisations with an annual turnover of more than $3M.[49]
Australian Financial Services License **Regulator:** Australian Securities and Investments Commission (ASIC) **Regulation:** *Corporations Act 2001* and associated regulations	Australian Financial Service (AFS) licensees must have adequate financial, technological and human resources and must adequately manage cybersecurity risks as part of their licence obligations. Adequate technological systems, policies and procedures must be in place to ensure sensitive consumer information is protected and to minimise the risk of consumer harm. ASIC takes enforcement action when an AFS licensee does not meet these obligations. This includes having adequate risk management systems to manage cybersecurity risks.[50] [51]
Consumer Data Right (CDR) **Regulators:** Australian Competition and Consumer Commission (ACCC) jointly with the OAIC **Regulation:** Competition and Consumer Act 2010 (CCA)	The CDR, under the CCA, is an opt-in service that provides consumers with improved access to, and control over, their data and enables sharing of data with accredited third parties. The CDR applies in the banking and energy sectors with non-bank lending to follow as a third sector. The CDR is jointly administered by the OAIC and the ACCC. The ACCC is responsible for accreditation and the OAIC is responsible for regulating privacy and confidentiality under the CDR. The CDR regime is maintained by 13 privacy safeguards contained in the Competition and Consumer Act 2010 and supplemented by the Consumer Data Rules enforced by the OAIC.

49 In October 2023, the Federal Government agreed to adopt 38 proposals, with in-principle support on a further 68 proposals pending further impact analysis and consultation following the release of the Privacy Act Review Report in February 2023.

50 An AFS licensee, RI Advice, was found to have breached its license obligations to act effectively and fairly when it failed to have adequate risk management systems to manage its cybersecurity risks. See Footnote 24 above.

51 The ASIC Market Integrity Rules also impose obligations on market operators and participants to have technological and operational resilience.

Continuous disclosure **Regulator**: Australian Securities Exchange (ASX) **Regulation** *ASX Listing Rules, ASX Listing Rule 3.1, Guidance Note 8*	Entities listed on ASX are subject to continuous disclosure obligations under the ASX Listing Rules. This means that any information that has a material effect on the price or value of an entities' securities must be disclosed. As a general rule, data breaches that would reasonably be expected to have a material effect on the price of a listed entity's securities are required to be disclosed to the ASX.[52]
Energy Sector Framework **Regulator/Administrator:** Australian Energy Market Operator (AEMO) **Regulation/Framework:** *Australian Energy Sector Cyber Security Framework (AESCF)*	The AESCF is an energy sector industry framework developed by the AEMO, industry participants and governance agencies, including ACSC. It is designed as a tool to assess cyber maturity and promote uplift in capability and cyber resilience. The ASCF leverages existing international standards frameworks, including NIST, ISO 27001 and the US department of energy's electricity Subsector Cybersecurity Capability Maturity Model.
Financial Services **Regulator:** Australian Prudential Regulation Authority (APRA) **Legislation:** *Australian Prudential Regulation Authority Act 1998, Banking Act 1959, Superannuation Industry (Supervision) Act 1993, Insurance Act 1973, Life Insurance Act 1995 and Private Health Insurance (Prudential Supervision) Act 2015*	Cross industry Standards apply to APRA-regulated entities authorised deposit-taking institutions, general insurers, life companies private health insurers and registrable superannuation entities.
Regulation: *CPS 220 (Risk Management)*	CPS 220 requires all APRA-regulated entities to have systems for identifying, measuring, evaluating, monitoring, reporting, and controlling or mitigating material risks that may affect its ability, or the ability of the group it heads, to meet its obligations to depositors and/or policyholders. The Board of an APRA-regulated entity is ultimately responsible for having a risk management framework that is appropriate to its size, business mix and complexity.

52 See also Footnote 39 above.

Regulation: *CPS 234 (Information Security)*	CPS 234 aims to ensure APRA-regulated entities take measures to be resilient against information security incidents, including cyberattacks, by maintaining an information security capability commensurate with information security vulnerabilities and threats. A key objective of CPS 234 is to minimise the likelihood and impact of information security incidents on the confidentiality, integrity or availability of information assets, including information assets managed by related parties or third parties. The Board of an APRA-regulated entity is ultimately responsible for ensuring that the entity maintains its information security.
Regulation: *CPS 230 (Operational Risk Management)*[53]	CPS 230 will require APRA-regulated entities to prepare for service disruptions by understanding the impacts of these events on customers and the wider financial system, take action to prevent these and enhance their operational resilience. It has three main objectives: strengthening operational risk management through requirements to address identified weaknesses in existing controls, improving business continuity planning to ensure regulated entities are positioned to respond to severe disruptions, and enhancing third-party risk management by ensuring risks from material service providers are appropriately managed. The Board of an APRA-regulated entity is ultimately accountable for oversight of an entity's operational risk management. This includes business continuity and the management of service provider arrangements.
Regulation: *CPS 231 (Outsourcing) and CPS 232 (Business Continuity Management)*[54]	CPS 231 requires all outsourcing arrangements involving material business activities entered into by an APRA-regulated institution be subject to appropriate due diligence, approval and ongoing monitoring and all risks arising from outsourcing material business activities are appropriately managed. CPS 232 requires APRA-regulated institutions to implement a whole-of-business approach to business continuity management that is appropriate to the nature and scale of the operations to increase resilience to business disruption arising from internal and external events and may reduce the impact on an institution's business operations, reputation, profitability, depositors, policyholders and other stakeholders. The Board of an APRA-regulated entity has ultimate responsibility for the outsourcing policy of the entity.
Health Records **Regulator/Administrator:** Australian Digital Health Agency, OAIC (data breaches) **Regulation:** *My Health Records Act 2012*	The My Health record system is designed to facilitate access by healthcare recipients and treating healthcare providers, to a summary of health information about a healthcare recipient. The system requires that organisations take reasonable steps to protect healthcare identifiers from misuse and loss, and unauthorised access, modification or disclosure. The supporting My Health records rules set out the security requirements that participating organisations must comply with to be eligible to be registered and to remain registered under the My Health record system. The system also requires a participating organisation to notify the OAIC of any data breaches.

53 From 1 July 2025. CPS 230 will replace: Prudential Standard CPS 231 Outsourcing (CPS 231), Prudential Standard CPS 232 Business Continuity Management (CPS 232), Prudential Standard SPS 231 Outsourcing (SPS 231), Prudential Standard SPS 232 Business Continuity Management (SPS 232) and Prudential Standard HPS 231 Outsourcing (HPS 231).

54 See Footnote 47 above.

Public sector **Regulator/Administrator:** Department of Home Affairs **Regulation/Framework:** *Protective Security Policy Framework* (PSPF)	The PSPF applies to non-corporate Commonwealth entities subject to the Public Governance, Performance and Accountability Act 2013 (PGPA Act) to the extent consistent with legislation. The PSPF represents better practice for corporate Commonwealth entities and wholly-owned Commonwealth companies under the PGPA Act.
Security of critical infrastructure (SOCI) **Regulator/Administrator:** Department of Home Affairs **Regulation:** *Security of Critical Infrastructure Act 2018*	The SOCI Act places obligations on responsible entities for certain critical infrastructure assets in 11 relevant critical infrastructure sectors. The regime imposes three positive security obligations that can apply to all critical infrastructure assets, depending on their asset class: to provide operational and ownership information to the Register of Critical Infrastructure Assets, to report cyber incidents which impact the delivery of essential services to the ACSC and to adopt, maintain and comply with a written risk management program. There are enhanced cyber security obligations for assets deemed as Systems of National Significance.

Emerging regulatory areas

Cyber security is a fast-moving area and there are areas which organisations and their leaders should monitor for developments. They include:

Privacy

The *Privacy Act Review Report* released in February 2023 recommended a number of significant changes including the introduction of more prescriptive privacy rules, greater alignment with EU data protection laws, a specific focus on online services, and the empowerment of regulators to play a more active enforcement role. As noted above the Federal Government agreed to adopt 38 proposals, with in-principle support on a further 68 proposals pending further impact analysis and consultation. In practice, this means that the Government will likely implement privacy reforms in tranches, focusing initially on the 38 items it has indicated it 'agrees to', while conducting further engagement and impact assessments on the 68 'agreed in-principle' items. It also noted 10 recommendations, which may mean there will be no further immediate action.

The Government's response indicates the key areas for reform are: bringing the Privacy Act into the digital age, uplifting protections, increasing clarity and simplicity for entities and individuals, improving individuals' control and transparency over their personal information and strengthening enforcement. At this stage, the small business and employee records exemption remains but the Government is likely to consult on this area earlier rather than later.[55]

Australian Cyber Security Strategy 2023 – 2030 and *2023 – 2030 Australian Cyber Security Action Plan*

Released by the Federal Government in November 2023, the *2023-2030 Australian Cyber Security Strategy* and the accompanying *2023-2030 Australian Cyber Security Action Plan*, which supplements the Strategy sets out the key cyber security initiatives to be delivered over the next two years. These documents outline significant proposed legislative reforms to introduce six cyber shields:

- A no-fault, no-liability *ransomware* reporting obligation for businesses
- *Amendments to data retention requirements* focusing on non-personal data to address the burden and risks relating to entities holding significant amounts of data for longer than necessary
- *Further amendments to the SOCI Act* to subject telecommunications providers to stronger cyber reporting requirements by moving security regulation for this sector from the Telecommunications Act 1997 to the SOCI Act and clarifying and increasing cyber obligations for sectors including managed service providers, aviation, maritime and offshore facility regulated entities
- *An enhanced Government review and remedy power,* and
- *A last resort all hazards consequence management power* where Government would be able to authorise action to manage the consequences of a nationally significant incident.[56]

Artificial intelligence (AI)

On 26 March 2024, the Senate resolved to establish the Select Committee on Adopting Artificial Intelligence (AI), to inquire into and report on the opportunities and impacts for Australia arising out of the uptake of AI technologies in Australia. The Terms of Reference of the Committee can be found here. The Committee is anticipated to present its final report in September 2024. The Committee will consider international approaches to regulate AI activities, such as the European AI Act - the first of its kind - that aims to regulate high-risk activities. The EU AI Act classifies AI according to its risk so that unacceptable risk is prohibited with most of the law addressing high-risk AI systems, which are regulated. A smaller section handles limited-risk AI systems, which are subject to lighter transparency obligations. Developers and deployers must ensure that end-users are aware that they are interacting with AI for example, chatbots and deepfakes. In the EU, the majority of obligations fall on developers of high-risk AI systems including those that intend to market or put into service high-risk AI systems in the EU, regardless of whether they are based in the EU or another country, as well as on other foreign providers where the high-risk AI system's output is used in the EU. Most other jurisdictions have taken a guardrail approach to regulating deployers of AI through Codes of Conduct, tools and guidance and model AI Governance Frameworks.

55 For further detail see The long road to Australian privacy reform, Minter Ellison, 5 October 2023 and Federal Government signals broad support for significant Privacy Act reforms, Allens, 12 October 2023.

56 For further information see *Australia's Cyber Security Strategy for 2023 – 2030 is here*, Gilbert & Tobin, 28 November 2023

The Australian Government published its interim response to its consultation on supporting responsible AI discussion paper in January 2024. Principles guiding the Australian Government's interim response to support safe and responsible AI include the following:

- a risk-based approach
- balanced and proportionate to business innovation
- collaborative and transparent
- a trusted international partner, and
- a community-first approach

The proposed approach and next steps relate to preventing harm from occurring through testing, transparency and accountability, clarifying and strengthening laws to safeguard citizens, working internationally to support the safe development and deployment of AI and maximising AI's benefits.

9. Standards, Frameworks and Certifications

As noted in Section 4, organisations should consider the benefits and costs of adopting the standards below, in addition to, or alignment with, any applicable legislative requirements.

Cyber Risk Management and Cyber Security

- NIST Cybersecurity Framework and NIST 800-53
- Essential 8
- Information Security Manual (ISM)
- Microsoft Secure Score
- MITRE ATT&CK
- *CIS Critical Security Controls*
- *Cloud Security Alliance Cloud Controls Matrix*
- *Open Web Application Security Project (OWASP) Top 10*

International Standards (IT)

- *ISO/IEC 27001:2022 Information security, cyber security and privacy protection – Information security management systems – Requirements*
- *ISO 28000:2033 Security and resilience – Security Management systems – Requirements*
- *ISO/IEC 38500:2024 Information Technology – Governance of IT for the organization*

International Standard (Risk)

- *ISO 31000:2018 Risk Management – Guidelines*

International Standard (Business Continuity)

- *ISO 22301:2019 Business Continuity Management Systems – Requirements*

Australian Commonwealth Government Entities

- *Protective Security Policy Framework (PSPF)*

APRA-regulated entities:

- *CPS 220 Risk Management*
- *CPS 230 Operational Risk Management*
- *CPS 234 Information Security*

Payment card processing:

- *Payment Card Industry Data Security Standard* (PCI DSS)

10. Resources

Reporting to government

- Australian Cyber Security Hotline on 1300 CYBER1 (1300 292 371)
- Report a cybercrime, incident or vulnerability to the Australian Signals Directorate

Privacy

- Office of the Australian Information Commissioner (OAIC)
- Guide to conducting privacy impact assessments Guide to undertaking privacy impact assessments, OAIC
- Notifiable data breaches, OAIC

Cyber Resilience and Security Guidance

- Cyber resilience, ASIC
- Australian Cyber Security Centre, Australian Signals Directorate
- Security Guidance
- Cyber and Infrastructure Security Centre (CISC)
- Overview of Cyber Security Obligations for Corporate Leaders (CISC)

Charities

- Australian Charities and Not-for-profits Commission Governance Toolkit Cyber Security

Scams

- Scamwatch – ACCC

International

- NIST https://www.nist.gov/cybersecurityhttps://www.nist.gov/cybersecurityISO .gov/cybersecurity
- NIST Cyber Security Framework 2.0

11. International Regulations

Jurisdiction	Legislation/Regulation
Canada	There are three general forms of law regulating security and privacy in Canada: • The Federal *Personal Information Protection and Electronic Documents Act (PIPEDA)* which regulates and enforces privacy policy for both public and private organisations, except in cases where there is a provincial equivalent that meets the same minimum standard as PIPEDA (such as PIPA in Alberta). The legislation does not currently include mandatory disclosure of data breaches or provide for any penalties. • The provincial variant of PIPEDA in Alberta the *Personal Information Protection Act (PIPA)* which requires organisations to take measures to protect data and includes mandatory disclosure of data breaches and information leaks. • Various health information acts, such as the *Health Information Protection Act* which protects private health information. Only three provinces have legislation that protects health information, Ontario, New Brunswick and Newfoundland. PIPEDA applies to employee information only in connection with a Federal works, undertakings, or businesses (FWUB), whereas the provincial PIPA applies to provincially regulated private sector organisations.[57]
European Union EU)	The General Data Protection Regulation (GDPR) came into effect in May 2018 are considered the highest standard of privacy and security law globally. While passed in the EU the GDPR imposes obligations on organisations anywhere, provided they target or collect data related to people in the EU. There is an ability to levy significant fines for breach of its privacy and security standards. A number of countries have used the GDPR as a model. Key terms to be aware of include: personal data, data processing, data subject, data controller and data processor. Notably the GDPR includes a 'right to erasure', a right of the subject of the data to request erasure of personal data related to them on a range of grounds.
Singapore	The 2018 *Cybersecurity Act* establishes a legal framework for the oversight and maintenance of national cybersecurity in Singapore. Its four key objectives are to: • Strengthen the protection of Critical Information Infrastructure against cyber-attacks. • Authorise CSA to prevent and respond to cybersecurity threats and incidents. • Establish a framework for sharing cybersecurity information. • Establish a light-touch licensing framework for cybersecurity service providers.

57 See Cybersecurity laws and regulations in Canada, Kate Callegari

Jurisdiction	Legislation/Regulation
United Kingdom	There is no overarching, primary national cybersecurity law, there are four critical legislative schemes that govern cybersecurity, data privacy, and data protection in the UK: • The *Data Protection Act 2018* • The UK General Data Protection Regulation passed following the UK's exit from the EU • The *Network and Information Security Regulations 2018* • The *Computer Misuse Act 1990* Other relevant pieces of legislation relating to cyber security in the UK include the *Telecommunications (Security) Act 2021, the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016* and the *Privacy and Electronic Communications Regulations.* Many UK organisations have also adopted other global cyber security regulations and frameworks like the PCI Security Standards Council, NIST, SOX, and the US Health Insurance Portability and Accountability requirements.
United States of America	Cybersecurity regulation in the United States is divided between federal and state laws. The Federal Trade Commission (FTC) is responsible for enforcing cybersecurity regulations and legislation at the federal level. In addition, the Department of Homeland Security (DHS) and the NIST also have roles in regulating cybersecurity. The primary law governing cybersecurity in the United States is the Federal Trade Commission Act (FTCA). This law prohibits deceptive acts and practices in business, including those related to data security. The FTC also enforces the Gramm-Leach-Bliley Act (GLB), which requires companies to protect the customer data they collect. Currently, 47 states and the District of Columbia have passed their own cyber security laws. These laws range from breach notification laws to data privacy regulations. California has the most comprehensive cybersecurity laws, with the California Consumer Privacy Act providing residents greater control over their data. Since December 2023, large US Securities and Exchange public companies must comply with a new set of cybersecurity disclosure rules aimed to enhance disclosure of cybersecurity incidents and increase visibility into cybersecurity governance. The new disclosure regime requires disclosures of material cybersecurity incidents immediately after they occur and periodic disclosure of a company's cybersecurity efforts and improvements.[58]

58 See *The SEC's new cybersecurity disclosure rules decoded: what they mean for investors*, Jonathan D. Uslaner and Jimmy Brunetto, 1 June 2024.

12. Acronyms and Glossaries

- ACSC – Australian Cyber Security Centre
- APRA – Australian Prudential Regulation Authority
- APT – advanced persistent threat
- ASD – Australian Signals Directorate
- BEC – business email compromise
- CCPA – California Consumer Protection Act (US)
- CISO – Chief Information Security Officer
- DDoS – Distributed Denial of Service attack
- DLP – data loss prevention
- E8 – Essential Eight
- EDR – endpoint detection and response
- GDPR – General Data Protection Regulation (Europe)
- HIPAA – Health Insurance Portability and Accountability Act (US)
- ICT – Information and communications technology
- IOT – 'internet of things'
- MFA – multifactor authentication
- MSP – managed service provider
- MSSP – Managed security service provider
- NIST – National Institute of Standards and Technology Cyber Security Framework (US)
- PCI DSS – Payment Card Industry Data Security Standards
- RBAC – roles-based access controls
- RPO – recovery point objective
- RTO – recovery time objective
- SIEM – security information and event management
- SOC – security operations centre
- SOCI – Security of Critical Infrastructure
- SOX – Sarbanes-Oxley Act (US)
- SSO – single sign-on
- XDR – Extended detection and response

Glossaries of cybersecurity terms:

- ACSC
- ISM
- SANS
- NIST
- Cybrary
- US National Initiative for Cybersecurity Careers and Studies

13. References

Reports

- *2022-2030 Cyber Threat Trends for Critical Infrastructure*, Australian Signals Directorate.
- *2023-2023 Cyber Security Strategy*, Australian Government and 2023 – 2030 Cyber Security Action Plan, Australian Government.
- *ASD Cyber Threat Report 2022-2023*, Australian Signals Directorate Australian Cyber Security Centre.
- *Cyber Insurance: Protecting our way of life, in a digital world*, Insurance Council of Australia.
- *The Global Risks Report 2024,* 19th Edition, World Economic Forum.
- *Allianz Risk Barometer Identifying the major business risks for 2024*, Allianz Commercial.
- *Information Risk Insights Study 2022*, Cyentia Institute.
- *REP 716 Cyber resilience of firms in Australia's financial markets: 2020–21*, ASIC.

Guides

- *Good Governance Guide Cyber Security*, Governance Institute of Australia.
- *Key questions for an organisation's board of directors*, ASIC.
- *Risk Management for Directors: A Guide*, 2nd edition, Governance Institute of Australia.

Articles

- *ASIC to target boards, execs for cyber failures*, Australian Financial Review, 19 September 2023.
- *How much cybersecurity expertise does a board need?*, CSO, 25 October 2023.
- *Cyber in 2023 and 2024: What we've seen and what's to come,* Governance Directions, Governance Institute of Australia, 1 February 2024.
- *Cyber risk: Be prepared*, ASIC, 15 July 2022.
- *Cyber safety a company culture matter*, ASIC, 10 June 2022.

Other

- *Interim Policy and Supervision Priorities Update*, Letter to All APRA-regulated entities, 31 January 2024.

Governance Institute of Australia

Governance Institute of Australia
GPO Box 1594,
Sydney NSW 2001
1800 251 849
www.governanceinstitute.com.au