

# ASFA Financial Crimes Protection Initiative

## Cyber Security Toolkit



# Contents

1. Introduction	3
CEO Foreword	5
About the contributors	7
Overview	8
2. Snapshot: Cyber Security Legislation relevant to Australian Superannuation Funds	10
3. Incident Response Planning & Management	13
Toolkit: Summary of Advised Outcomes in Cyber Preparedness Planning	20
Toolkit: Indicative Reporting Timeframes	23
6. Snapshot: Sources of Obligations	24
7. Snapshot: Overarching Obligations	26
8. Obligations Map	27
9. Additional Resources	29

**The Association of Superannuation Funds of Australia Limited (ASFA)**

PO Box 1485, Sydney NSW 2001

T +61 2 9264 9300 or 1800 812 798 (outside Sydney)

ABN 29 002 786 290

ACN 002 786 290

This material is copyright. Apart from any fair dealing for the purpose of private study, research, criticism or review as permitted under the Copyright Act, no part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without prior written permission.

Enquiries are to be made to The Association of Superannuation Funds of Australia Limited.

[www.superannuation.asn.au](http://www.superannuation.asn.au)

© ASFA 2024

# Introduction

The Association of Superannuation Funds of Australia (ASFA) is the voice of superannuation. Operating since 1962, we represent over 100 organisations, including corporate, industry, retail, and public sector funds, as well as critical service providers. ASFA unites the superannuation community, supporting our members with research, advocacy, education and collaboration to help Australians enjoy a dignified retirement. We promote effective practice and advocate for efficiency, sustainability and trust in our world-class retirement income system.

ASFA proudly represents 90 per cent of all 17 million Australians with superannuation. With over \$4 trillion in retirement savings under management, the superannuation system carries a significant responsibility, one that must be matched by strong regulatory compliance and operational resilience.

ASFA has made multiple submissions to government consultations on Australia's cyber security laws, including with respect to the Government's National Cyber Security Strategy 2023-2030, and the comprehensive Cyber Security Legislative Package 2024.

ASFA will always fight for the best possible cyber security protections for those with superannuation, knowing that a trusted superannuation system is good for all Australians.

This Cyber Security Toolkit is a product of ASFA's Financial Crimes Protection Initiative, launched in September 2024. This toolkit brings together key legal obligations and prudential expectations that apply to superannuation trustees in relation to cyber security.

It draws on relevant legislation and guidance to help superannuation trustees and their customers understand their legal obligations when it comes to cyber security.

Together, these frameworks set out the regulatory expectations for trustees in protecting member data and maintaining operational integrity. This toolkit is intended to simplify, aggregate and explain existing laws and guidance and act as a practical resource for trustees and service providers. It is designed to consolidate the regulatory requirements that apply to cyber resilience in the superannuation sector, and to assist users in interpreting and applying them in day-to-day operations.

It does not constitute legal advice, should not be relied upon as such, and superannuation fund trustees should seek their own independent advice regarding their rights and obligations.



The Commonwealth legislation drawn upon in creation of this toolkit includes the following:

1. Corporations Act 2001
2. Cyber Security Act 2024
3. Financial Accountability Regime Act 2023 and associated rules
4. Privacy Act 1988
5. Security of Critical Infrastructure Act 2018
6. Superannuation Industry (Supervision) Act 1993  
Other APRA requirements and guidance relied upon includes:
7. CPS 230 Operational Risk Management
8. CPS 234 Information Security
9. SPS 220 Risk Management
10. SPS 510 Governance
11. Prudential Practice Guide CPG 234 on Information Security, and
12. Prudential Practice Guide CPG 235 on Managing Data Risks
13. Prudential Practice Guide CPG 230 Operational Risk Management
14. Prudential Practice Guide SPG 220 Risk Management.

The toolkit is designed to simplify, aggregate and explain the relevant laws and guidance. It is not legal advice and should not be relied upon as such. Superannuation funds and their service providers should obtain independent advice in relation to their specific obligations.

ASFA acknowledges the contribution of Mills Oakley, whose support and legal expertise in reviewing the content of this toolkit has helped ensure its accuracy and relevance for industry users.

ASFA provides this resource to support stronger compliance and promote a consistent approach to cyber resilience across the superannuation sector.



## CEO Foreword

# Mary Delahunty

Australians trust superannuation with their future. That trust is hard-earned, and the superannuation industry must be unwavering in its commitment to meeting it.

---

Every person with super places their trust in a system that is built for the long term. It is our job to ensure that system remains resilient, well-governed, and prepared to meet evolving risks, including those posed by cyber threats.

Cybersecurity is now a core responsibility for superannuation trustees. The scale and sensitivity of the data we hold, and the critical role super plays in the financial lives of Australians means that the stakes are high. Our protections must be robust. Our systems must be tested. Our response plans must be ready.

ASFA is committed to supporting the sector with the tools and clarity needed to meet these obligations. This Cyber Security Toolkit is part of that commitment. It draws together the relevant legislation and regulatory guidance to help trustees understand and manage their responsibilities.

Our role is to support a superannuation system that Australians can rely on, not only for performance, but for protection. That responsibility is shared across the system, and it is one we all must uphold with care and diligence.

Thank you for your continued commitment to strengthening the security and sustainability of Australia's superannuation system.

**Mary Delahunty**  
ASFA CEO

# About the contributors



## **Mitch Riley-Meijer**

*Incident Response Manager | Cyber Risk & Insurance*

Mitch is a nationally recognised cyber security expert with 15 years of experience in national security, cyber risk management, and incident response. Before joining Mills Oakley, he coordinated whole-of-government cyber incident management at the National Office of Cyber Security, working with Critical Infrastructure operators on major incidents.



## **Jason Symons**

*Partner | Cyber Risk & Insurance*

Jason is a specialist cyber risk and insurance lawyer. Jason's team advises organisations on cyber and privacy risk management, data governance, cyber incident response, data breach reporting, malicious financial fraud, and insurance coverage of relevant costs and liability, and represents clients in regulatory investigations and litigation arising from cyber events.



## **Mark Bland**

*Partner | Financial Services*

Mark provides advisory and transactional services to financial institutions, including superannuation trustees, fund managers, financial advisers, and licence holders. With five years at ASIC, he specialises in regulatory affairs, compliance advice, and responses to enforcement actions. His expertise covers AFS and RSE licensee obligations, applications, conduct, and disclosure.



## **Sebastian Reinehr**

*Senior Advisor | ASFA*

Sebastian Reinehr is a Senior Adviser at ASFA. He has extensive policy expertise related to combatting cybersecurity threats and financial crime. He previously served as Policy Director at the Australian Finance Industry Association and as an Adviser and Senior Adviser to the Opposition Leader and senior Cabinet and Shadow Cabinet Ministers.





# Overview

## About this toolkit

The escalating risk of cyber incidents poses significant security challenges for trustees of superannuation funds and their service providers. Effective cyber security risk management, and preparing to respond to cyber security incidents, is crucial at all levels of management, starting from the Board. The Board, Directors, and senior management are instrumental in establishing robust frameworks to identify and mitigate cyber risks.

Australia's cyber security regulatory framework is evolving to keep pace with the modern cyber environment. Increasingly, the Australian Government and courts are introducing new requirements for corporate leaders to be informed about these threats, and to have adequate processes in place to address incidents where they occur. Key legislative obligations under the Superannuation Industry (Supervision) Act 1993, the Privacy Act 1988, and the Corporations Act 2001, mandate businesses to prepare for, report, and respond to cyber incidents. Trustees also have relevant obligations under prudential standards, including Prudential Standard CPS 234 Information Security and CPS 230 Operational Risk Management, replacing SPS 231 Outsourcing and SPS 232 Business Continuity Management on 1 July 2025.

However, the expectations surrounding cyber preparedness often lack clarity. Industry feedback indicates a need for clearer guidance on what constitutes effective cyber security.

This toolkit is designed to support Boards, Company Directors, Chief Executive Officers, and other corporate leaders navigate important obligations and requirements that should be considered in developing comprehensive cyber security response plans for superannuation funds.

While primarily aimed at senior leaders, the toolkit is also valuable for officers at all organisational levels. It should be used alongside other best practice frameworks, including those from the Association of Super Funds Australia.

This toolkit serves as an initial guide to Australia's cyber security regulatory landscape. However, it is essential for funds to seek specialised legal and technical support to address the complexities of the modern cyber environment relevant to them and to fully understand their evolving obligations.

## Role of the Board and Senior Management

The Board is ultimately responsible for the sound and prudent management of an RSE licensee's business operations. This includes accountability for approving the risk appetite for information security and cyber risk, overseeing cybersecurity frameworks, ensuring compliance with the relevant law and ensuring that there are adequate personnel and systems in place to manage cyber risks and incidents.

The Board plays a crucial role in overseeing cyber security within a Fund. This responsibility involves understanding and managing cyber risks, ensuring that the Fund has robust cyber security policies and practices in place, and actively engaging with the executive team, particularly domain experts such as the Chief Information Security Officer (CISO), Chief Information Officer (CIO) or Chief Technology Officer (CTO).

Further, the Board must ensure that cyber security is integrated into the overall enterprise risk management framework and that there is a clear strategy for addressing potential threats. This includes regular updates on the company's cyber security posture, understanding the implications of new technologies, and ensuring compliance with relevant laws and regulations.

Cyber security encompasses several high-level domains, including risk and vulnerability management, network security, identity and access management, and incident response. These domains collectively aim to protect the organisation's information systems from various threats, such as data breaches, malware, and phishing attacks. Effective cyber security requires a comprehensive and holistic approach that includes risk assessment, threat intelligence, and continuous monitoring to detect and respond to potential incidents.

When it comes to cyber response and response preparedness, the Board's role extends to ensuring that the Fund has appropriate governance, processes and key decision support mechanisms in place, in the form of a response plan. This plan should outline the steps to be taken in the event of a cyber incident, including communication protocols, roles and responsibilities, and recovery procedures. The Board must oversee the testing and updating of this plan to ensure its effectiveness. During an incident, the Board provides strategic guidance and ensures that management is addressing all aspects of the breach, from mitigating immediate threats to managing long-term impacts on the company's reputation and operations.

## General Disclaimer

Each cyber incident is inherently unique and may give rise to distinct legal and operational considerations depending on the specific circumstances of your organisation. The information provided herein is of a general nature only and is not intended to constitute legal advice. You should obtain independent legal advice tailored to your particular situation and seek guidance from appropriately qualified professionals.



# Snapshot: Cyber Security Legislation relevant to Australian Superannuation Funds

## Australian Commonwealth Laws & Standards

Superannuation Funds may wish to consider the applicability of the following laws and legislated standards, and consider your comprehensive compliance strategy to ensure adherence with (but not limited to):

Privacy Act 1988 (Cth) (Privacy Act)	
Applicability	Australian Government agencies and organisations with an annual turnover of more than \$3 million or with an Australian financial services (AFS) licence. Certain other entities may be subject to requirements depending on business operations.
Summary	The Privacy Act regulates how personal information is handled by Australian Government agencies and organisations with an annual turnover of more than \$3 million and all AFS licensees. It includes 13 Australian Privacy Principles that set standards for the collection, use, storage, and disclosure of personal information. Ensuring compliance with the Privacy Act requires implementation of robust data protection measures and provides for reporting obligations detailed in the Notifiable Data Breach Scheme.
Administering Body	Office of the Australian Information Commissioner
More Information	<a href="#">Privacy Act</a>   <a href="#">OAIC</a>
Security of Critical Infrastructure Act 2018 (Cth) (SOCI Act)	
Applicability	Entities operating in any of the Critical Infrastructure Sectors that owns, operates, or has direct interests in a Critical Infrastructure Asset, which includes a Critical Superannuation Asset which is an asset of a fund with more than \$20 billion in assets.
Summary	The SOCI Act outlines the legal obligations for owners and operators of critical infrastructure assets across 11 key sectors, including communications, energy, and healthcare. It aims to enhance the resilience and security of Australia's critical infrastructure by managing risks and ensuring the continuity of essential services. Compliance with the SOCI Act involves identifying and managing risks associated with critical infrastructure assets. This is achieved through compliance with the Critical Infrastructure Risk Management Program and the Enhanced Cyber Security Obligations Framework.
Administering Body	Department of Home Affairs (Cyber and Infrastructure Security Centre)
More Information	<a href="#">Security of Critical Infrastructure Act 2018 (SOCI)</a>   <a href="#">CISC</a>
Cyber Security Act 2024 (Cth) (Cyber Act)	
Applicability	(Ransomware Reporting Obligations) Non-government entities with an annual turnover that exceeds the turnover threshold specified in the Rules.
Summary	The Cyber Act sets out mandatory reporting of ransomware payments for certain businesses and establishes a Cyber Incident Review Board to review significant cyber incidents.
Administering Body	Department of Home Affairs
More Information	<a href="#">Cyber Security Act</a>   <a href="#">Home Affairs</a>

Corporations Act 2001 (Cth) (Corporations Act)	
Applicability	Companies, directors and other officers, RSE licensees and Australian financial services licensees
Summary	The Corporations Act provides a uniform framework for company formation, governance, and insolvency in Australia. It regulates company responsibilities, including shareholder rights and directors' duties, ensuring transparency and accountability in corporate activities. The Corporations Act sets requirements for certain entities to submit notifications about 'reportable situations' (which may include among other matters significant data breaches) to the Australian Securities and Investments Commission.
Administering Body	Australian Securities and Investments Commission
More Information	<a href="#">Reportable situations</a>   <a href="#">ASIC</a>
Superannuation Industry (Supervision) Act 1993 (SIS Act)	
Applicability	RSE licensees, trustees of self-managed superannuation funds, RSE licensee and trustee directors
Summary	The SIS Act establishes the regulatory framework for superannuation funds in Australia to ensure they are operating prudently and in members' best financial interests. It applies to trustees of regulated superannuation entities that have elected to be regulated and are supervised by either APRA (for most large funds) or the ATO (for SMSFs). The SIS Act includes trustee and director covenants, including the requirements to exercise care, skill and diligence and to have robust risk management frameworks. It provides enforcement powers and penalties for non-compliance.
Administering Body	Australian Prudential Regulation Authority
More Information	<a href="#">Legislation for Superannuation Entities</a>   <a href="#">APRA</a>
Financial Accountability Regime Act 2023 (FAR Act)	
Applicability	Accountable entities (including RSE licensees) and accountable persons
Summary	The FAR Act establishes a framework requiring accountable entities to follow several broad obligations including to conduct its business with honesty and integrity, and with due skill, care and diligence. Accountable entities are required to appoint and register accountable persons that collectively cover all areas of the business operations of the accountable entity and its relevant group. The regulator rules prescribe certain key functions for inclusion in the FAR register. Key Functions relevant to cyber security include scam management; data management; technology management; and training and monitoring of relevant staff.
Administering Body	Australian Prudential Regulation Authority and Australian Securities and Investments Commission
More Information	<a href="#">RG 279 Financial Accountability Regime: Information for accountable entities</a>

Prudential Standard CPS 234—Information Security (CPS234)	
Applicability	APRA-regulated entities.
Summary	CPS234 establishes requirements for APRA-regulated entities to minimise the likelihood and impact of information security incidents on the confidentiality, integrity or availability of information assets, including those managed by related or third parties. It sets obligations for entities to report an information security incident that materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers. It also sets obligations for regulated entities to report incidents that have been reported to other regulators in a timely manner.
Administering Body	Australian Prudential Regulation Authority
More Information	<a href="#">CPS 234 Information Security   Prudential Handbook   APRA</a>
Prudential Standard CPS 230 —Operational Risk Management (CPS230)	
Applicability	APRA-regulated entities.
Summary	CPS230 requires APRA-regulated entities to identify, assess, and manage operational risks through robust internal controls, continuous monitoring, and remediation. A key requirement is the development and maintenance of a Business Continuity Plan (BCP) that ensures critical operations can continue within predefined tolerance levels during disruptions. The standard also requires entities to manage risks associated with service providers by implementing a comprehensive service provider management policy, establishing formal agreements, and conducting rigorous oversight.
Administering Body	Australian Prudential Regulation Authority
More Information	<a href="#">CPS 230 Operational Risk Management   Prudential Handbook   APRA</a>
Prudential Standard SPS 220—Risk Management (SPS220)	
Applicability	APRA-regulated entities.
Summary	SPS220 establishes requirements for APRA-regulated entities to maintain a risk management framework that covers all material risks, including information security and cyber security risks. The framework must be consistent with the entity's strategic objectives and business plan. It sets obligations for Boards of regulated entities to approve a risk management strategy, business plan and risk appetite statement as part of a risk management framework that is appropriate to the size, business mix and complexity of the entity.  It also sets obligations for regulated entities to notify APRA when they become aware of a significant breach of, or material deviation from, the risk management framework, or that the risk management framework does not adequately address a material risk, including material information security and cyber security risks.
Administering Body	Australian Prudential Regulation Authority
More Information	<a href="#">SPS 220 Risk Management   Prudential Handbook   APRA</a>

## ASX Continuous Disclosure Obligations

ASX-listed entities are required to comply with the continuous disclosure obligations under ASX Listing Rule 3.1, that if they become aware of information that a reasonable person would expect to have a material effect on the price or value of its securities, it must immediately notify the ASX (subject to any exception in Listing Rule 3.1A that may apply). This can include data breaches and other types of cyber security incidents.

This assists to maintain the integrity and efficiency of Australian markets that trade in ASX quoted securities or derivatives of those securities by ensuring that the market is properly informed. While most RSE licensees are not ASX-listed entities they may form a part of group that is ASX-listed and therefore should be aware of the ASX disclosure obligations.

# Incident Response Planning & Management

## What is a Cyber Security Incident

The definition of a cyber security incident can be sourced from multiple locations, both for its definition originating from the technical cyber security community and originating from various pieces of legislation within Australia.

The Cyber Act gives us the legislated definition of a cyber security incident as being:

- (1) One or more acts, events or circumstances:
  - (a) of a kind covered by the meaning of cyber security incident in the Security of Critical Infrastructure Act 2018; or
  - (b) involving unauthorised impairment of electronic communication to or from a computer, within the meaning of that phrase in that Act, but as if that phrase did not exclude the mere interception of any such communication.

Whereas the SOCI Act defines a cyber security incident as being:


One or more acts, events or circumstances involving any of the following:

- (a) unauthorised access to:
  - (i) computer data; or
  - (ii) a computer program;
- (b) unauthorised modification of:
  - (i) computer data; or
  - (ii) a computer program;
- (c) unauthorised impairment of electronic communication to or from a computer;
- (d) unauthorised impairment of the availability, reliability, security or operation of:
  - (i) a computer; or
  - (ii) computer data; or
  - (iii) a computer program.

From a technical community perspective, the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) defines a cyber security incident as:

*An unwanted or unexpected cybersecurity event, or a series of such events, that either has compromised business operations or has a significant probability of compromising business operations.*

This terminology above differs from the definitions of 'cybercrime', and it is important to understand the differences between the two, particularly for the purposes of



responding to either and understanding which obligations may apply in a given circumstance, depending on whether you are responding to a cyber security incident, or cybercrime.

The Attorney-General's Department (Commonwealth), defines cybercrime as being either:

- Cyber-dependent crimes that are directed at Information Communications Technologies (ICT) infrastructure and other forms ICT. This includes crimes such as denial of service, ransomware and data breaches.
- Cyber-enabled crimes, such as online fraud and identity crimes, which can increase in their scale and or/reach through the use of ICT.

Cyber-dependent crimes exist only in the digital world, whereas cyber-enabled crimes are traditional crimes committed in new ways.

Cybercriminals can range from individuals to criminal networks through to politically motivated or state-sponsored actors.

The motivations for cybercrime can vary significantly, including financial gain, interpersonal conflict, causing societal disruption, or gaining a competitive edge, through to being ideologically or politically motivated.

For the purposes of this toolkit, we interpret the definition of a cyber security incident being:

One or more acts, events or circumstances that result in the unauthorised access to, modification of, or impairment of the availability, reliability, security or operation of a computer, computer data, or a computer program, irrespective of the potential that those acts, events or circumstances could potentially result in cybercrime.

Cyber security incidents can take many forms, but generally observed a cyber security incident could be:

- A denial or disruption of digital services;
- Unauthorised access to secure network resources, data or controlled physical spaces holding ICT infrastructure;
- Loss of confidentiality of information, including data breaches, spills and leaks;
- Introduction of malicious code, software or vulnerability into a controlled environment;
- Cyber-enabled extortion or ransomware;
- Social engineering fraud, using techniques such as phishing, spear phishing and whaling, and (but not limited to);
- Identity theft and fraud.



## Cyber Preparedness Planning & Incident Response Plans

Cyber Preparedness Planning refers to the strategic practice of ensuring an organisation can prevent, respond to, and recover from cyber incidents. This involves a fund-wide effort, not just the responsibility of the IT or security team.

Creating an effective Cyber Incident Response Plan (CIRP) involves several key steps, often guided by frameworks such as those from the National Institute of Standards and Technology (NIST) or the Escal Institute of Advanced Technologies (SANS). These are explored in more detail in the next part of this document.

The process begins with preparation, where a specific committee or group, comprised of senior executives from multiple disciplines (including legal, HR and operations teams) is established with clear roles and responsibilities. This committee or group should report directly to the Board, ensuring all relevant personnel are trained and aware of their duties during an incident.

There is no defined composition for this group, but at a minimum, it is advised that it include:

- Chief Executive Officer, or equivalent, as the Chair of the committee;
- Cyber Incident Manager, as the manager and facilitator of the response efforts;
- General Counsel, supported by specialist external legal counsel;
- Internal/External Auditors;
- Chief Risk Officer;
- Chief Technology Officer;
- Chief Information Security Officer (if separate from the CTO function);
- Chief Finance Officer;
- Chief HR Officer;
- Chief Communications Officer;
- Company Secretary; and
- Management, record keepers and administrative support staff.

The role of the Board in this process is pivotal. Boards must elevate cyber risk from a technical issue to a strategic risk, ensuring it is integrated into the overall risk management framework.



## Incident Response vs Incident Management

Incident Response is a structured process aimed at identifying, managing, and mitigating the effects of cyber security incidents to minimise damage, recover operations, and prevent future occurrences.

It involves a series of coordinated efforts from specialised teams using frameworks, tools, and processes designed to address cyber security incidents effectively.

The SANS Institute, an internationally recognised leader in information security, cyber security training and response frameworks, provides a framework for Incident Response:

1. Preparation - This involves setting up and maintaining an incident response capability. This includes developing policies, procedures, and tools, conducting risk assessments, and forming an incident response team.
2. Identification - In this phase, the organisation detects and determines whether an incident has occurred. This involves monitoring systems for unusual activity and gathering evidence to understand the nature and scope of the incident.
3. Containment - The aim here is to limit the damage and prevent the incident from spreading. This can involve short-term containment measures, such as isolating affected systems, and long-term containment strategies to restore normal operations while ensuring the threat is neutralised.
4. Eradication - This step focuses on removing the cause of the incident, such as deleting malware and closing vulnerabilities. It also involves identifying the root cause to prevent future incidents.
5. Recovery - In this phase, systems are restored to normal operation. This includes validating that affected systems are clean, monitoring for any signs of weakness, and ensuring that business operations can resume safely.
6. Lessons Learned (or Review) - After the incident is resolved, the organisation reviews and analyses the incident to improve future response efforts. This involves documenting what happened, how it was handled, and identifying areas for improvement.





Figure 1: SANS Incident Response Framework

Incident Management, on the other hand, encompasses a broader scope. It involves managing incidents that exceed the capabilities of an internal Security Operations Centre (SOC) and Incident Response teams, generally requiring involvement by Senior Executive and, potentially, the Board.

Incident Management focuses on the overall coordination and management of significant incidents, ensuring that they are handled efficiently and effectively. It includes the same six steps as Incident Response but also involves higher-level strategic planning and coordination.

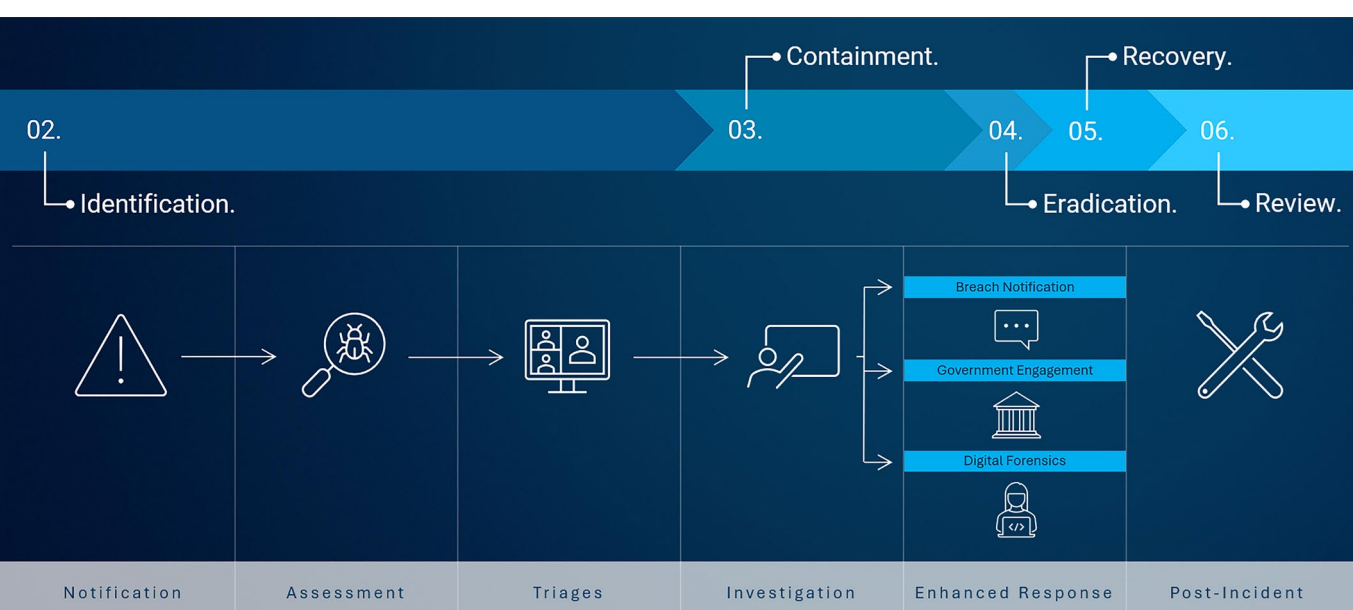


Figure 2: Mills Oakley Cyber Incident Management Lifecycle



## The Importance of External Legal Counsel as Cyber Incident Response Managers

Engaging external legal counsel as ‘cyber incident response managers’ is crucial for several reasons, especially within the Australian corporate landscape. External legal counsel brings specialised knowledge and experience in handling cyber incidents, which may not be available in-house. Their expertise can be invaluable in navigating the complexities of a cyber incident and ensuring a swift and effective resolution.

One of the primary advantages is strengthening the claim of Legal Professional Privilege (LPP) protecting sensitive communications and documents from being disclosed in legal proceedings or regulatory investigations. This is particularly important given the increasing litigation and regulatory scrutiny following cyber incidents.

Moreover, external legal counsel ensures that the response to a cyber incident complies with relevant Australian laws and regulations highlighted in this toolkit. This compliance is essential to avoid penalties and maintain the organisation’s reputation. Legal experts also provide strategic advice on managing the incident, including communication with stakeholders, regulatory bodies, and the public, helping to mitigate reputational damage and ensure a coordinated and effective response.

In the event of subsequent legal actions, having external legal counsel involved from the outset ensures that the organisation is better prepared to defend itself. This includes managing evidence, conducting internal investigations, and preparing for potential class actions. APRA has stated in Prudential Standard SPS 510 Governance that the requirement for directors to have the necessary skills, knowledge and experience to understand the risks of an RSE licensee’s business operations and to ensure that the RSE licensee’s business operations are managed in an appropriate way taking into account these risks, does not preclude the Board from supplementing its skills and knowledge by engaging external consultants and experts.

## Leveraging Cyber Insurance to Support Incident Response

While cyber insurance products differ between insurers and brokers, coverage generally includes:

1. costs associated with incident response management, forensic investigation and data breach notification;
2. data restoration and reconstruction costs;
3. business interruption costs; and
4. indemnification of third-party liability claims and regulatory investigations; and
5. financial loss suffered as a result of social engineering fraud or theft due to unauthorised access.

Additionally, where a cyber insurance policy responds to cyber event involving ransomware or data extortion, where the event is due to the malicious acts of a foreign government actor or criminal gang, coverage may include costs related to:

1. the services of a ransom negotiator;
2. legal advice relating to any ransom demand; and
3. reimbursement of any ransom payment made.

Like traditional insurance products, cyber insurance uses price and risk selection to incentivise risk mitigation and minimise losses for policyholders. As part of the underwriting process, insurers often examine an organisation's cyber defences, identify vulnerabilities and provide guidance on how to strengthen cyber security. The uplift of the cyber security posture of an insured may be necessary to obtain cover or better terms.





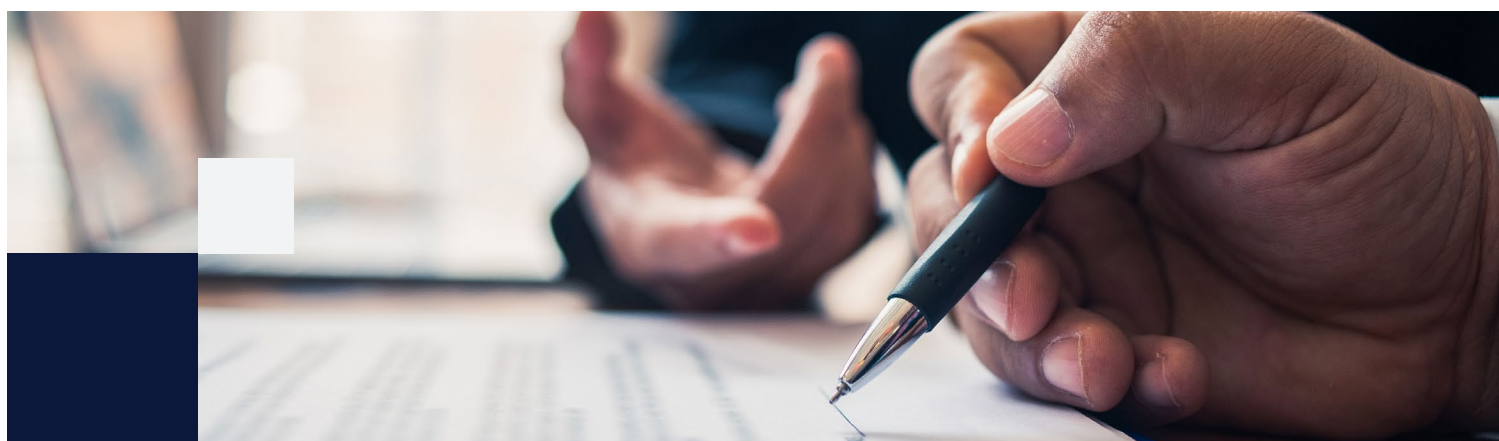
# Toolkit: Summary of Advised Outcomes in Cyber Preparedness Planning

Category	Advised Outcome	Key References	Specific Object Link
Governance & Oversight	Boards and executives ensure their CIRP is governed appropriately, with clear accountability for cyber risk management, response escalation, and oversight.	CPS234 Information Security	<a href="#">CPS234   Roles &amp; Responsibilities   Paras 13 &amp; 14</a>
		ISO 27001: A.6.1.1	<a href="#">ISO27001   Annex A   Control A.6.1.1</a>
		SPS220 Risk Management	<a href="#">SPS220   The Role of the Board   Paras 5 to 8</a>
		SPS 510 Governance	<a href="#">SPS 510   Role of the Board</a>
		CPS 230 Operational Risk Management	<a href="#">CPS 230 Roles and responsibilities Paras 20 to 23 and Para 58</a>
		Financial Accountability Regime Act 2023	<a href="#">Financial Accountability Regime Act 2023   Accountability obligations and Key Personnel obligations</a>
Regulatory Notifications	Regulatory bodies such as APRA, OAIC, and ASIC are notified within relevant required reporting timeframes of any reportable incidents involving data breaches or operational risks. <i>See: Checklist: Indicative Reporting Timeframes</i>	CPS234 Information Security	<a href="#">CPS234   APRA Notification   Paras 35 &amp; 36</a>
		Privacy Act (NDB Scheme)	<a href="#">The Privacy Act 1988   Division 3</a>
		RG104 AFS Licensing	<a href="#">RG104.29   Reporting on your Measures</a>
		CPS 230 Operational Risk Management	<a href="#">CPS 230   Notification Requirements   Paras 33, 42 and 59</a>
		Financial Accountability Regime Act 2023	<a href="#">Financial Accountability Regime Act 2023   Accountability obligations and Key Personnel obligations</a>
Stakeholder Communication	Crisis communication strategies ensure members, employers, staff, and external stakeholders receive timely, accurate information during a cyber incident.	OAIC Data Breach Guide	<a href="#">OAIC   Data Breach Preparation and Response</a>
		ISO 27035-4	<a href="#">ISO27035-4   Part 6   6.2 Communications</a>
		CPG234 Information Security	<a href="#">CPG234   Response to a Security Compromise   Paras 71 &amp; 72</a>
		CPS 230 Operational Risk Management	<a href="#">CPS 230   Communications Strategy   Para 40</a>
Incident Containment	The CIRP is supported by relevant technical processes, procedures and protocols (often termed 'Playbooks') to contain, isolate, and mitigate cyber threats to limit exposure and impact on critical 'crown jewels' systems, member services or sensitive data. The CIRP integrates these Playbooks by defining clear system-agnostic roles and responsibilities for key decision points, such as system isolation or shutdowns, in the event of a cyber incident.	ISO 27035-1; -2; -3	<a href="#">ISO27035-1   Principles and Process</a> <a href="#">ISO37035-2   Guidelines to Plan and prepare for Incident Response</a> <a href="#">ISO27035-3   Guidelines for ICT Incident Response Operations</a>
		NIST Cybersecurity Framework ID.AM; DE.CM; DE.AE; RS.MA; RS.AN; RS.CO; RS.MI	<a href="#">NIST   Cybersecurity Framework   Version 2.0</a>
		CPS234 Information Security	<a href="#">CPS234   Incident Management   Paras 23-26</a>

Category	Advised Outcome	Key References	Specific Object Link
Business Continuity	The fund maintains critical operations, including contributions, benefit payments, and member communications, even during cyber incidents.	CPS 230 Operational Risk Management	<a href="#">CPS 230   Business Continuity   Paras 34 to 46</a>
		ISO 22301	<a href="#">ISO22301   Business Continuity Management Systems</a>
		NIST Cybersecurity Framework RC.RP; RC.CO	<a href="#">NIST   Cybersecurity Framework   Version 2.0</a>
Member Protection	Controls ensure members' personal and financial data are safeguarded, and affected individuals are supported, including identity protection where necessary.	Privacy Act (as distinct from the NDB Scheme)	<a href="#">Federal Register of Legislation   The Privacy Act 1988</a>
		Privacy Act (NDB Scheme)	<a href="#">The Privacy Act 1988   Notification of eligible data breaches</a>
		CPS234 Information Security	<a href="#">CPS234   Information Security</a>
		ISO 27701	<a href="#">ISO27701   Privacy Extension for ISO27001/2</a>
		OAIC Data Breach Guide	<a href="#">OAIC   Data Breach Preparation and Response</a>
Root Cause Analysis	Post-incident analysis identifies vulnerabilities, threat vectors, and system/process failures, with remediation tracked and monitored.	ISO 27035	<a href="#">ISO27035-1   Principles &amp; Process</a> <a href="#">ISO27035-2   Guidelines to Plan and Prepare for Incident Response</a> <a href="#">ISO27035-3   Guidelines for ICT Incident Response Operations</a>
		NIST Cybersecurity Framework ID.AM; ID.RA; ID.IM; DE.AE; RS.AN; RS.CO; RS.MI; RC.CO	<a href="#">NIST   Cybersecurity Framework   Version 2.0</a>
		CPS234 Information Security	<a href="#">CPS234   Testing Control Effectiveness   Paras 27-34</a>
		SPS220 Risk Management	<a href="#">SPS220   Risk Management Declaration   Para 32</a>
		CPS 230 Operational Risk Management	<a href="#">CPS 230   Root cause identification   Para 31</a>
Lessons Learned	Insights gained from incidents feed into strategy updates, risk assessments, and training to improve organisational resilience.	ISO 27001: A.16.1.6	<a href="#">ISO27001   Annex A   Control A.16.1.6</a>
		ISO 27035	<a href="#">ISO27035-1   Principles &amp; Process   5.6 Learn Lessons</a> <a href="#">ISO27035-4   Coordination   5.6 Coordinated Learn Lessons</a>
		CPS234 Information Security	<a href="#">CPS234   Incident Management   Para 25(a) &amp; Paras 27-31</a>
		SPS220 Risk Management	<a href="#">SPS220   Risk Management</a>
Board Engagement	Boards receive structured, timely updates during and after incidents, ensuring effective decision-making and alignment with fiduciary and regulatory responsibilities.	CPS234 Information Security	<a href="#">CPS234   Roles &amp; Responsibilities   Paras 13 &amp; 14</a>
		SPS220 Risk Management	<a href="#">SPS220   The Role of the Board   Paras 5 to 8)</a>
		ASIC Cyber Resilience Good Practice Guide	<a href="#">ASIC   Good Practice Guide   Cyber Resilience</a>
		CPS 230 Operational Risk Management	<a href="#">CPS 230   Reporting   Paras 16, 27 and 58</a>
Reputational Management	Media, political, and stakeholder impacts are proactively managed to preserve member trust and public confidence in the fund's leadership and integrity.	ISO 22301	<a href="#">ISO22301   Support   7.4 Communication</a>
		OAIC Data Breach Guide	<a href="#">OAIC   Data Breach Preparation and Response</a>
		ASIC Cyber Resilience Good Practice Guide	<a href="#">ASIC   Good Practice Guide   Cyber Resilience</a>



Category	Advised Outcome	Key References	Specific Object Link
Recovery Readiness	The CIRP ensures a structured recovery, including restoration of data and systems and verification of their integrity before resuming full operations.	ISO 27031	<a href="#">ISO27031   Incident Response &amp; Business Continuity Planning</a>
		ISO 22301	<a href="#">ISO 22301   Operation   6.4 Business Continuity Plans &amp; Procedures</a>
		CPS234 Information Security	<a href="#">CPS234   Incident Management   Para 25(a)</a>
		NIST Cybersecurity Framework GV.RM; GV.RR; GV.PO; GV.OV; RC.RP	<a href="#">NIST   Cybersecurity Framework   Version 2.0</a>
		CPS 230 Operational Risk Management	<a href="#">CPS 230   Business Continuity   Paras 34 to 46</a>
Third-Party Risk Management	The CIRP accounts for risks associated with outsourced service providers (e.g. administrators, custodians), including vendor notification and coordination.	CPS234 Information Security	<a href="#">CPS234   Implementation of Controls   Para 22</a>
		CPS230 Operational Risk Management	<a href="#">CPS230   Management of service provider arrangements   Paras 47 to 60</a>
		ISO 27036-1; -2; -3	<a href="#">ISO27036-1   Cybersecurity-Supplier Relationships   Overview &amp; Concepts</a> <a href="#">ISO27036-2   Cybersecurity-Supplier Relationships   Requirements</a> <a href="#">ISO27036-3   Cybersecurity-Supplier Relationships   Supply Chain Security</a>
		OAIC Data Breach Guide	<a href="#">OAIC   Data Breach Preparation and Response</a>
Ongoing Improvement	The CIRP is updated regularly based on threat intelligence, test results, and evolving legal/regulatory requirements.	CPS234 Information Security Clause 22	<a href="#">CPS234   Testing Control Effectiveness   Para 31</a>
		ISO 27001 A.16.1.6	<a href="#">ISO27001   Annex A   Control A.16.1.6</a>
		NIST Cybersecurity Framework GV.RM; GV.RR; GV.PO; GV.OV; ID.AM; ID.RA; ID.IM; RC.RP	<a href="#">NIST   Cybersecurity Framework   Version 2.0</a>
		CPS 230 Operational Risk Management	<a href="#">CPS 230   Business Continuity Testing and Review   Paras 43 to 46</a>
		Financial Accountability Regime Act 2023	<a href="#">Financial Accountability Regime Act 2023   Accountability obligations and Key Personnel obligations</a>



# Toolkit: Summary of Indicative Reporting Timeframes

Source of Obligation	Obligation	Recipient	Timing	Relevant Tests & Assessments
Privacy Act	Notifiable Data Breach	OAIC	As soon as practicable*	<ul style="list-style-type: none"> <li>• Application &amp; Exemption</li> <li>• Credit Reporting, Credit Providers &amp; TFN Rule Tests</li> <li>• Impacted Information Type Assessments</li> <li>• Eligible Data Breach Test (inc. Serious Harm Test)</li> </ul> <p>* Entities must notify individuals as soon as practicable after completing the statement prepared for notifying the Commissioner (s 26WL(3)).</p>
SOCI Act	Mandatory Cyber Incident Reporting (Significant Impact)	CISC, via ReportCyber	Within 12 hours	<ul style="list-style-type: none"> <li>• Application &amp; Role of the Asset</li> <li>• Impact Assessment of the roles and responsibilities of the operator and owner of the asset</li> <li>• Impact Assessment of the role of the asset in the security incident</li> </ul>
SOCI Act	Mandatory Cyber Incident Reporting (Impacted Asset)	CISC, via ReportCyber	Within 72 hours	<ul style="list-style-type: none"> <li>• Application &amp; Role of the Asset</li> <li>• Impact Assessment of the roles and responsibilities of the operator and owner of the asset</li> <li>• Impact Assessment of the role of the asset in the security incident</li> </ul>
Cyber Act	Ransomware Payment Report	The Department of Home Affairs and ASD's ACSC, via ReportCyber	Within 72 hours	<ul style="list-style-type: none"> <li>• Application &amp; Exemption (inc. Critical Infrastructure Asset test)</li> <li>• Demand relation payment assessment</li> </ul>
Corporations Act	Reportable Situations	ASIC	Within 30 days	<ul style="list-style-type: none"> <li>• Application</li> <li>• Nature of the Situation or Investigation</li> <li>• Significance &amp; Material Impact</li> </ul>
CPS234	Information Security Incident	APRA	Within 72 hours	<ul style="list-style-type: none"> <li>• Application &amp; Material Impact (inc. potential)</li> <li>• Notification to other regulators</li> </ul>
CPS234	Security Control Weakness	APRA	Within 10 days	<ul style="list-style-type: none"> <li>• Application &amp; Material Impact (inc. potential)</li> </ul>
CPS 230	Operational Risk Incident	APRA	Within 72 hours	<ul style="list-style-type: none"> <li>• Material Financial Impact or material impact on the ability of the entity to maintain critical operations</li> </ul>
CPS 230	Disruption to Critical Operation	APRA	Within 24 hours	<ul style="list-style-type: none"> <li>• Disruption outside tolerance</li> </ul>
CPS 230	Service Provider Agreement	APRA	Within 20 business days	<ul style="list-style-type: none"> <li>• Entering into or materially changing an agreement for the provision of a service on which the entity relies to undertake a critical operation</li> <li>• Entering into or significantly changing any material offshoring arrangement</li> </ul>

Funds and their service providers should also consider their contractual obligations to report cyber incidents, which may differ from legislated timeframes.

## Snapshot: Sources of Obligations

The obligations relating to an RSE licensee's incident response arise from multiple sources, including. Depending on the nature and scope of the incident, organisations may be required to report breaches to regulatory authorities, notify affected individuals and take remedial actions to prevent recurrence.

### Privacy Act 1988

**Type:** Legislation | **Applicability:** Organisations with an annual turnover more than \$3 million | **(Privacy Act)**

Notifiable Data Breach Scheme

Under the Notifiable Data Breach Scheme any organisation or agency the Privacy Act 1988 covers must notify affected individuals and the Office of the Australian Information Commissioner when a data breach is likely to result in serious harm to an individual whose personal information is involved.

**Source:** Privacy Act – Part IIIC Division 3

### Security of Critical Infrastructure Act 2018

**Type:** Legislation | **Applicability:** Critical Infrastructure Asset Operators | **(SOCI Act)**

Mandatory Cyber Incident Reporting

Critical infrastructure owners and operators are required to report a cyber security incident if they are captured by the critical infrastructure asset definitions and that incident is having, had, or is likely to have, an impact on the critical infrastructure asset.

**Source:** Security of Critical Infrastructure Act – Part 2B

### Cyber Security Act 2024

**Type:** Legislation | **Applicability:** Organisations with an annual turnover more than \$3 million | **(Cyber Act)**

Ransomware Payment Reporting

A reporting business entity must make a report within 72 hours of making the ransomware payment (or becoming aware that the ransomware payment has been made).

**Source:** Cyber Security Act – Part 3

### Financial Accountability Regime Act 2023

**Type:** Legislation | **Applicability:** Accountable Entities including RSE Licensees | **(FAR Act)**

Appointment of Accountable Persons

An accountable entity must comply with its accountability obligations and appoint responsible persons that are responsible for Key Functions of the accountable entity. Key functions relevant for cyber security include scam management, data management, technology management, and training and monitoring of relevant staff.

**Source:** FAR Act – Chapter 2

## Corporations Act 2001

**Type:** Legislation | **Applicability:** Australian Financial Services & Australian Credit Licensees | **(Corporations Act)**

Reportable Situations

Australian financial service licensees and Australian credit licensees are required to notify ASIC of all reportable situations.

**Source:** Corporations Act – Part 7.6 Division 3

## Financial Accountability Regime Act 2023

**Type:** Legislation | **Applicability:** Accountable Entities including RSE Licensees | **(FAR Act)**

Appointment of Accountable Persons

An accountable entity must comply with its accountability obligations and appoint accountable persons that are responsible for Key Functions of the accountable entity. Key functions relevant for cyber security include scam management, data management, technology management, and training and monitoring of relevant staff.

**Source:** FAR Act – Chapter 2

## Prudential Standard CPS 234

**Type:** Standard | **Applicability:** APRA-regulated entities | **(CPS234)**

Notification of a Security Incident

As a support to SPS 220 Risk Management, CPS 234 requires an entity to manage its information security. Entities must have policies, controls and incident management plans. Entities must notify APRA of any information security incidents.

**Source:** CPS234 Information Security – APRA Notification

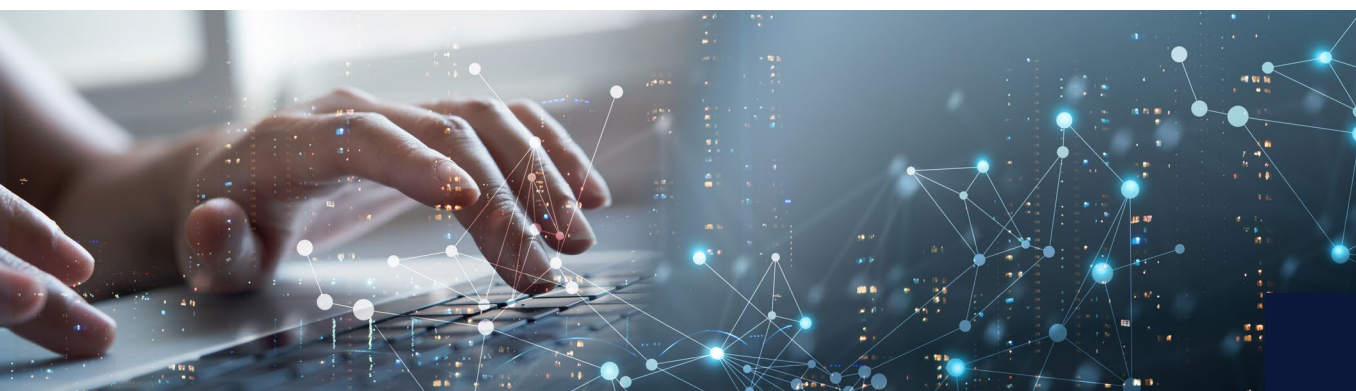
## Prudential Standard CPS 234

**Type:** Standard | **Applicability:** APRA-regulated entities | **(CPS234)**

Notification of a Information Security Control Weakness

As a support to SPS 220 Risk Management, CPS 234 requires an entity to manage its information security. Entities must have policies, controls and incident management plans. Entities must notify APRA of any information security incidents.

**Source:** CPS234 Information Security – APRA Notification



## Corporations Act 2001

**Type:** Legislation | **Applicability:** Australian Financial Services Licensees | **(Corporations Act)**

Licence Obligations

Australian financial service licensees must act efficiently, honestly and fairly and (if an RSE licensee also acts as a responsible entity of a registered scheme) have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the licence.

**Source:** Corporations Act – Part 7.6 Division 1 – Sections 912A(1)(a), (d) and (h)

## Corporations Act 2001

**Type:** Legislation | **Applicability:** Directors and officers of a corporation | **(Corporations Act)**

Directors' and Officers' Duties

Directors and Officers have duties to act with care and diligence, to act in good faith and in the best interests of the company, to avoid conflicts of interest, and to not improperly use their position or information to gain an advantage or cause harm.

**Source:** Corporations Act – Chapter 2D – Sections 180 to 184

## Superannuation Industry (Supervision) Act 1991

**Type:** Legislation | **Applicability:** Corporate Trustee & Director of a Corporate Trustee | **(SIS Act)**

Trustee Covenants

A Trustee must exercise the same degree of care, skill and diligence as a prudent superannuation trustee would exercise.

**Source:** SIS Act – Part 6 – Section 52(2)(b) and 52A(2)(b)

## Prudential Standard SPS 510

**Type:** Standard | **Applicability:** APRA-regulated entities | **(SPS510)**

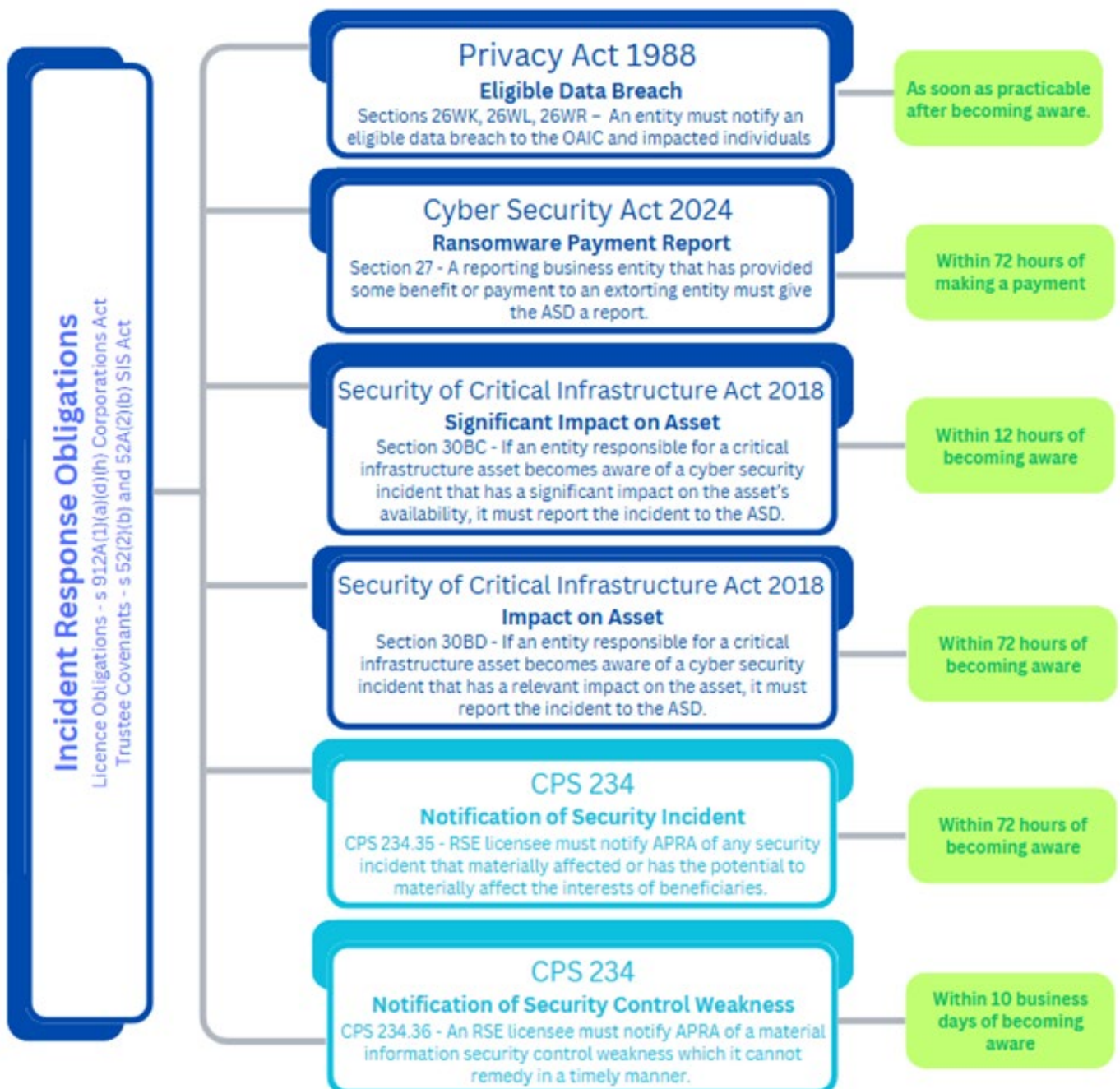
Responsibility of the Board and Delegation

The Board has ultimate responsibility for oversight of the sound and prudent management of an APRA-regulated entity. In fulfilling its functions the Board may delegate authority to management to act on behalf of the Board.

**Source:** SPS510 Governance – The Board and senior management

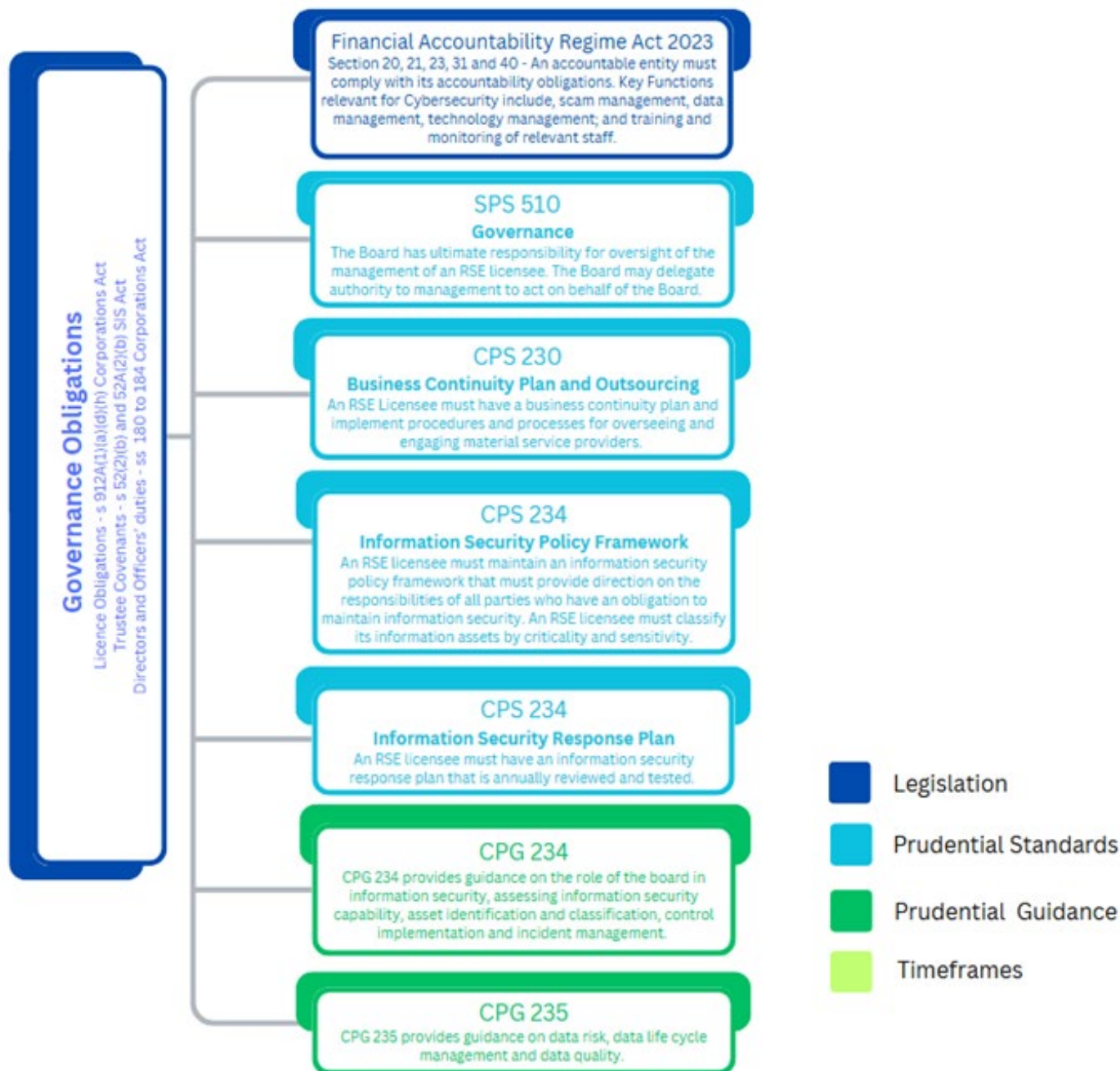


# Obligations Map



\* Before considering the timeframes above please consider the Relevant Tests and Assessments in the Indicative Reporting Timeframes Checklist on page 22.







## Additional Resources

**AICD** – [Cyber Security Governance Principles](#). This document outlines best practices and frameworks for boards to enhance cyber resilience and manage cyber risks effectively.

**APRA** – [Improving Cyber Resilience and the Role of the Board](#). APRA emphasises the critical role of boards in overseeing and strengthening cyber resilience within financial institutions.

**ASIC** – [Key Questions for an Organisations' Board of Directors](#). ASIC provides essential questions that boards should ask to ensure robust cyber risk management and resilience.

**ASIC** – [Good Practices in Cyber Resilience](#). This guide highlights effective practices for organisations to enhance their cyber resilience through strategic governance and risk management.

**ASD's ACSC** – [ReportCyber Portal](#). The ReportCyber portal allows individuals and organisations to report cyber incidents and access resources for cyber threat awareness.

**ASD's ACSC** – [Cyber Security Resources for Business and Government](#). This resource offers comprehensive cyber security guidelines and tools for businesses and government entities to protect against cyber threats.

**CISC** – [Guidance Materials for SOCI Act, Enhanced Cyber Security Obligations and Mandatory Cyber Reporting](#). This guidance details the enhanced cyber security obligations for critical infrastructure assets under the SOCI Act.

**OAIC** – [About the Notifiable Data Breaches Scheme](#). The NDB scheme requires organisations to notify affected individuals and the OAIC when a data breach is likely to result in serious harm.

**OAIC** – [Australian Privacy Principles Guidelines](#). These guidelines explain the mandatory requirements of the Australian Privacy Principles and how they apply to organisations covered by the Privacy Act.



ASFA Financial Crimes Protection Initiative  
Cyber Security Toolkit