Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Cyber Incident Response Plan Guidance and Template

December 2021

cyber.gov.au

About this document

Context

The Australian Government defines cyber security as measures used to protect the confidentiality, integrity and availability of systems and information. A cyber incident is an unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations.[1]

Australian organisations are targeted by malicious cyber adversaries. The Australian Cyber Security Centre's (ACSC) assessment is malicious cyber activity against Australia's national and economic interests is increasing in frequency, scale, and sophistication. As adversaries become more adept, the likelihood and severity of cyber attacks is also increasing due to the interconnectivity and availability of information technology platforms, devices and systems exposed to the internet.

To illustrate the volume of cyber incidents occurring in Australia, the ACSC responded to over 1500 cyber security incidents between 1 July 2020 and 30 June 2021.[2] While many of the incidents reported to the ACSC could have been avoided or mitigated by good cyber security practices, such as implementation of ASD's Essential Eight security controls, risks will still remain when organisations operate online.

Managing responses to cyber incidents is the responsibility of each affected organisation. All organisations should have a cyber incident response plan to ensure an effective response and prompt recovery in the event security controls don't prevent an incident occurring. This plan should be tested and regularly reviewed.

To be effective, a cyber incident response plan should align with the organisation's incident, emergency, crisis and business continuity arrangements, as well as jurisdictional and national cyber and emergency arrangements. It should support personnel to fulfil their roles by outlining their responsibilities and all legal and regulatory obligations.

While organisations are responsible for managing incidents affecting their business, Australia's Cyber Incident Management Arrangements (CIMA) outline the inter-jurisdictional coordination arrangements and principles for Australian governments' cooperation in response to national cyber incidents.[3]

Purpose

The Cyber Incident Response Plan (CIRP) Template and the Cyber Incident Response Readiness Checklist (Appendix B) are intended to be used as a starting point for organisations to develop their own plan and readiness checklist.

Each organisation's CIRP and checklist need to be tailored according to their unique operating environment, priorities, resources and obligations.

In addition to a CIRP, organisations can develop more detailed, day-to-day procedures to supplement the cyber incident response plan. This could include more detailed playbooks to aide response to common incident types, such as ransomware or data breaches, and standard operating procedures (SOPs) to respond to incidents affecting specific assets.

[1] Australian Cyber Security Centre, cyber.gov.au, 'Glossary', accessed 16 December 2020.
[2] Australian Cyber Security Centre, cyber.gov.au, ACSC Annual Cyber Threat Report 1 July 2020 to 30 June 2021.
[3] Cyber Incident Management Arrangements for Australian Governments (CIMA), December 2018.

Acknowledgements

This document was created by the ACSC using multiple resources. The ACSC acknowledges the following resources used to develop this template:

- The Australian Government Information Security Manual (ISM).
- Australian Prudential Regulation Authority (APRA) Prudential Practice Guide CPG 234 Information Security June 2019 (https://www.apra.gov.au/sites/default/files/cpg_234_information_security_june_2019_1.pdf).
- A Cyber Incident Response Plan template developed by efforts of the Australian Energy Sector Readiness and Resilience Working Group in 2019, specifically with support from the Australian Energy Market Operator (AEMO), Tasmanian Department of State Growth, the Victorian Government Department of Premier and Cabinet and the ACSC.
- Victorian Government Incident Response Plan template 2019 (https://www.vic.gov.au/prepare-cyber-incident).
- Queensland Government Enterprise Architecture Incident management guideline 2018 (https://www.qgcio.qld.gov.au/documents/incident-management-guideline).
- United States National Institute of Standards and Technology (NIST) Special Publication 800-61 Revision 2 Computer Security Incident Handling Guide 2012 (https://www.nist.gov/privacy-framework/nist-sp-800-61).
- International Organisation for Standardisation standards:
    - ISO/IEC 27035-1, *Information technology – Security techniques – Information security incident management, Part 1 Principles of incident management,*
    - ISO/IEC 27035-2, *Information technology – Security techniques – Information security incident management, Part 2 Guidelines to plan and prepare for incident response*,
    - ISO/IEC 27035-3, *Information technology – Information security incident management, Part 3 Guidelines for ICT incident response operations.*
- Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Incident & Vulnerability Response Playbooks (https://us-cert.cisa.gov/ncas/current-activity/2021/11/16/new-federal-government-cybersecurity-incident-and-vulnerability).

Questions and Feedback

Questions and feedback about this document should be directed to ASD Assist via email at ASD.Assist@defence.gov.au or phone at 1300 CYBER1 (1300 292 371).

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Cyber Incident Response Plan Template

How to use this template

This section is structured as a template with guidance to support development of an organisation's own CIRP.

This template is not exhaustive. Each organisation's CIRP should be tailored according to its unique operating environment, priorities, resources and obligations.

Remove this box and other instructions before finalising your plan.

Insert an appropriate security classification for your plan.

Table of Contents

1. Authority and Review

Include information about the document owner, document reviewer, approver, version control and date of next review or other thresholds to review the plan. For example, a plan could be reviewed on a bi-annual or annual basis, and following a cyber incident, a cyber security exercise, or following organisational changes or changes to policies and other plans, or changes to legislation, regulation or jurisdictional arrangements.

For example:

Document Control and Review

Document Control	
Author	
Owner	
Date created	
Last reviewed by	
Last date reviewed	
Endorsed by and date	
Next review due date	

Version Control

Version	**Date of Approval**	**Approved By**	**Description of Change**
0.1			Initial Draft

2. Purpose and Objectives

Include the purpose and objectives of the CIRP. For example:

Purpose of the CIRP (Example)

To support a swift and effective response to cyber incidents aligned with the organisation's security and business objectives.

Objectives of the CIRP (Examples)

1. To provide guidance on the steps required to respond to cyber incidents.
2. To outline the roles, responsibilities, accountabilities and authorities of personnel and teams required to manage responses to cyber incidents.
3. To outline legal and regulatory compliance requirements for cyber incidents.
4. To outline internal and external communication processes when responding to cyber incidents.
5. To provide guidance on post incident activities to support continuous improvement.

3. Standards and Frameworks

Include the relevant standards and frameworks used to inform your organisation's CIRP. For example:

- State/territory government standards and frameworks
- National standards and frameworks (e.g. Australian Government Information Security Manual, Australian Prudential Regulation Authority (APRA) Prudential Practice Guide CPG 234 Information Security)
- Industry standards and frameworks (e.g. Australian Energy Sector Cyber Security Framework)
- International standards and frameworks
    - NIST Computer Security Incident Handling Guide
    - International Standard ISO/IEC27035-1
    - International Standard ISO/IEC 27035-2
    - International Standard ISO/IEC 27035-3

4. High Level Incident Response Process

Include a summary of your organisation's incident response process.

For example:

5. Common Security Incidents and Responses

Include commonly used terms and their definitions used in your organisation. A list of commonly used terms and definitions is provided at Appendix A.

5.1. Common Threat Vectors

Include a summary of common threat vectors for your organisation.

The following table contains common threat vectors from the NIST Computer Security Incident Handling Guide.

Type	Description
External/Removable Media	An attack executed from removable media or a peripheral device (e.g. malicious code spreading onto a system from an infected USB flash drive).
Attrition	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g. a DDoS intended to impair or deny access to a service or application or a brute force attack against an authentication mechanism, such as passwords).
Web	An attack executed from a website or web-based application (e.g. a cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware).
Email	An attack executed via an email message or attachment (e.g. exploit code disguised as an attached document or a link to a malicious website in the body of an email).
Supply Chain Interdiction	An antagonistic attack on hardware or software assets utilising physical implants, Trojans or backdoors, by intercepting and modifying an asset in transit from the vendor or retailer.
Impersonation	An attack involving replacement of something benign with something malicious (e.g. spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation).
Improper usage	Any incident resulting from violation of an organisation's acceptable usage policies by an authorised user, excluding the above categories (e.g. a user installs file sharing software, leading to the loss of sensitive data).
Loss or Theft of Equipment	The loss or theft of a computing device or media used by an organisation (e.g. a laptop, smartphone or authentication token).

5.2. Common Cyber Incidents

Include a summary of common cyber incident types and the initial response activities.

The following table provides a list of common cyber incident types and space to include your organisation's corresponding initial response activities, which form the typical minimum response.

Type/Description	**Response** *Briefly describe the response, for example, notify relevant individuals, activate cyber incident response plan, isolate affected devices, follow relevant playbook*
Ransomware: a tool used to lock or encrypt victims' files until a ransom is paid.	
Malware: a Trojan, virus, worm, or any other malicious software that can harm a computer system or network.	
Denial of Service (DoS) and Distributed Denial of Service (DDoS): overwhelming a service with traffic, sometimes impacting availability.	
Phishing: deceptive messaging designed to elicit users' sensitive information (such as banking logins or business login credentials) or used to execute malicious code to enable remote access.	
Data breach: unauthorised access and disclosure of information.	
Industrial Control System compromise: unauthorised access to ICS.	

6. Roles and Responsibilities

Include details of the roles and responsibilities of core individuals and teams responsible for incident response and decision making.

As a minimum, include the personnel responsible for receiving the initial notification, the operational level Cyber Incident Response Team (CIRT) and the strategic level Senior Executive Management Team (SEMT).

All personnel listed here should be familiar with their responsibilities in this plan and practise their response.

6.1. Points of Contact for Reporting Cyber Incidents

Include details about primary and secondary (backup) internal points of contact for your staff or stakeholders to report cyber incidents to over a 24/7 period.

Example table:

Name	Hours of Operation	Contact Details	Role Title	Responsibilities

6.2. Cyber Incident Response Team (CIRT)

Include details of the CIRT responsible for managing responses to cyber incidents.

The composition of your CIRT will vary depending on the size of your organisation and available skills and resources.

Include details of any 3rd party vendors that provide or manage your ICT systems/applications. If applicable, include details of your external incident response providers and the services they provide.

Example table:

Name	Organisation Role	Contact Details	CIRT Role Title	CIRT Responsibilities
			Cyber Incident Manager	• Response planning • CIRT Operations
			Deputy Cyber Incident Manager	• Situational analysis • Threat intelligence • Technical advice
			Security Manager	• Investigation (if suspected internal threat) • Law enforcement liaison
			Incident Responder	• Technical investigation (e.g. collection and processing of network and host data) • Containment, remediation and recovery efforts • Investigation findings report
			Communications, engagement and media advisor	• Information and warnings • Internal communications • Media and community liaison/spokesperson

Other CIRT roles could include system administrators, network engineers, auditing and change requests.

For more significant cyber security incidents the CIRT could be expanded to include:

Name	Organisation Role	Contact Details	CIRT Role Title	CIRT Responsibilities
			Business continuity advisor	• Facilities support • Business and community consequence analysis/management
			Legal advisor	• Legal advisory services (incl. regulatory compliance)
			Finance and procurement advisor	• Facilities and finance support
			Administration and record keeping	• Administration support, incl. Incident Log, Evidence and Situation Reporting

16.2.1. Surge Arrangements

Include your process for implementing surge arrangements to involve any or all of the following, and are to be selected dependent on the nature of the incident and resourcing required:

- People
- Hardware and software
- Financial resources

6.3. Senior Executive Management Team (SEMT)

Significant cyber incidents may require the formation of the SEMT to provide strategic oversight, direction and support to the CIRT, with a focus on:

- Strategic issues identification and management
- Stakeholder engagement and communications (including Board and ministerial liaison, if applicable)
- Resource and capability demand (including urgent logistics or finance requirements, and human resources considerations during response effort).

Include details of the SEMT responsible for managing responses to cyber incidents.

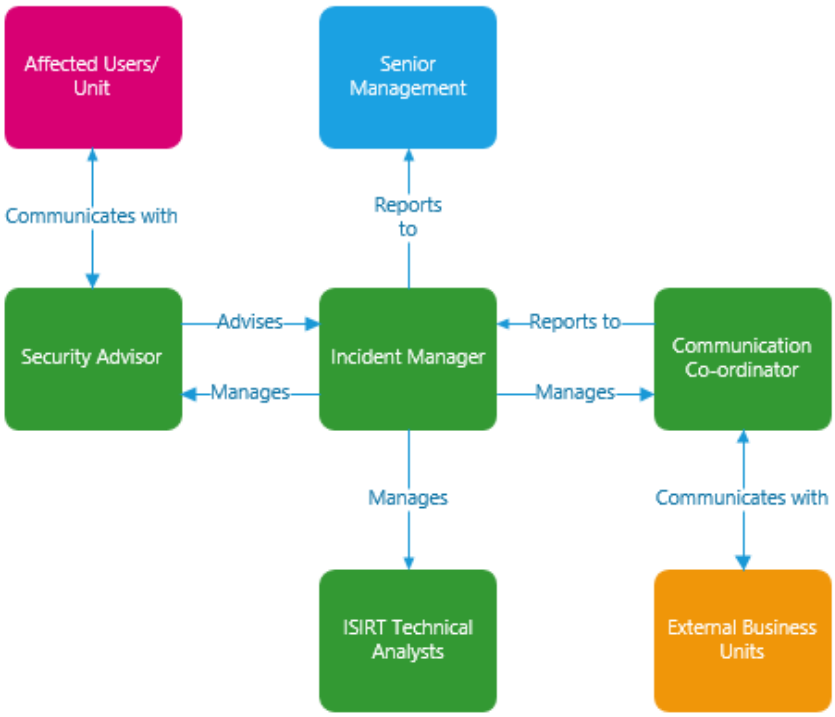
The composition and roles of your SEMT may vary depending on the incident impacts and size and structure of your organisation.

Name	Contact Details	Title	SEMT Role
		Chief Executive Officer	• SEMT Chair
		Chief Information Officer	• SEMT Deputy Chair

		Chief Information Security Officer	• SEMT Deputy
		Chief Operating Officer	• Operational functions of the business
		Chief Financial Officer/ Procurement Manager	• Emergency procurement and expenditure oversight
		Legal Council	• Regulatory compliance, cyber insurance
		Media and Communications Manager	• Public relations and stakeholder engagement
		People and Culture Manager	• Staff welfare management

6.4. Roles and Relationships

Include a diagram picturing the relationship between the key personnel and teams involved in the response. Here is an example from the Queensland Incident Management Guideline (September 2018).



*ISIRT stands for Information Security Incident Response Team.

7. Communications

Include your organisation's process for managing internal and external communications.

Include how your organisation is prepared to:

- Support the CIRT and SEMT communications requirements
- Respond to potential increase in internal and external enquiries or complaints about the incident or the effects
    - How will the customer helpdesk manage enquiries and be supported?
    - How will the IT Helpdesk (or equivalent) manage enquiries and be supported?
    - What communication channels are available to affected customers and staff (e.g. telephone hotline, information on the website or social media)?
- Communicate publicly about the incident, including to the public and the media
    - Who has the primary responsibility for authorising and speaking on behalf of the organisation? How will this person be supported?
    - Who has responsibility for producing and approving information for release to the public and media?
- Monitor news media, social media and other forms of media and use it to support communications.

Include details for backup communication channels to communicate with staff and stakeholders.

7.1. Internal Communications

Include your organisation's process and expected timeframes to communicate relevant incident information to your staff (for example customer service team, the Board, senior executives, and staff affected).

In your internal messaging consider how you can inform staff about the incident and support business continuity. Consider providing:

- A brief summary of the incident and business impact
- Actions currently being undertaken to resolve the incident
- Actions staff can take to assist
- Business continuity options for staff who are affected by the incident
- Messaging for external stakeholders
- Key points of contact for enquiries
- Expected timeframes for further updates.

7.2. External Communications

Include your organisation's process and timeframes to communicate relevant incident information to external stakeholders.

Depending on the impact and severity of the cyber incident, it may be necessary to communicate with external stakeholders, who may include:

- Stakeholders to support your incident response such as government agencies, third party incident response, law enforcement and/or sector organisations

- Stakeholders seeking information about the incident such as customers, government agencies, clients, shareholders, suppliers and/or sector organisations
- Media and the general public
- Other stakeholders, such as insurance providers.

In your external messaging consider how you can inform external stakeholders about the incident according to their role/interest. Consider:

- Information they need to know
    - System/services affected
    - Steps being taken to resolve the incident
    - Who your organisation is working with to support incident remediation
- Options for stakeholders affected by the incident (customers)
- Key points of contact for enquiries
- Expected timeframes for further updates.

Consider your organisation's approach to managing requests for information from interested sector and government groups following the incident for the purpose of sharing information and learning from your organisation's experience.

8. Supporting Procedures and Playbooks

8.1. Supporting Standard Operating Procedures (SOPs)

Include a list of supporting Standard Operating Procedures (SOPs) developed to support your organisation's incident response, and their physical and electronic locations. Examples of separate SOPs are:

- Event detection, triage and analysis
- Post event/incident detection or notification (i.e. actions taken after becoming aware of an event/incident)
- Incident detection, investigation and analysis
- Incident containment, remediation and recovery (such as when to observe and protect in place and when to implement remediation/mitigation strategies)
- Communications plan (internal and external)
- Emergency management plan
- Crisis management plan
- Business continuity plan
- Disaster recovery plan

8.2. Supporting Playbooks

Include a list of the supporting playbooks developed to provide step-by-step guidance for responses to common incidents, and their physical and electronic locations. Examples of supporting playbooks are:

- Cyber Security Incident Response Playbook – Phishing
- Cyber Security Incident Response Playbook – Data Breach/Theft
- Cyber Security Incident Response Playbook – Malware

- Cyber Security Incident Response Playbook – Ransomware
- Cyber Security Incident Response Playbook – Denial of Service

9. Sector, Jurisdictional and National Incident Response Arrangements

Include information about the relevant sector, state and/or territory, and national arrangements such as for notification, reporting and/or to seek support.

The CIRP could include a process chart of when to report incidents to relevant state, territory and federal agencies and/or seek assistance.

9.1. Sector Arrangements

Include information about the relevant sector arrangements, and your organisation's policy and process for implementing these arrangements.

9.2. Jurisdictional Arrangements

Each state and territory jurisdiction has its own cyber incident response arrangements. Organisations should contact the relevant government agency in their jurisdiction to understand the arrangements that apply, and include key information in the cyber incident response plan.

Include your organisation's position and process for reporting to and/or seeking assistance from state/territory law enforcement.

9.3. National Arrangements

Include your organisation's position and process for reporting to and/or seeking assistance from Australian Government agencies.

Australia's Cyber Incident Management Arrangements (CIMA) outlines the inter-jurisdictional coordination arrangements and principles for Australian governments' cooperation in response to national cyber incidents.

The CIMA (December 2018) can be viewed at https://www.cyber.gov.au/acsc/view-all-content/news/cyber-incident-management-arrangements-australian-governments.

Examples of potential national cyber incidents include:

- An organisation with links across multiple jurisdictions being compromised through a cyber incident
- Malicious cyber activity affecting critical national infrastructure where the consequences have the **potential** to cause sustained disruption of essential services or threaten national security
- Malicious cyber activity where the cause and potential extent of its geographic impact is uncertain, and
- A large-scale information system breach of sensitive data affecting persons or organisations in multiple jurisdictions.

The ACSC leads the Australian Government's response to cyber incidents. For information on how to report incidents to the ACSC, and to seek advice and assistance, visit the ACSC's website at https://www.cyber.gov.au/.

Appendix C provides the ACSC's incident triage questions.

10. Incident Notification and Reporting

Include your organisation's position as well as internal and external processes for incident notification and reporting.

Consider sector, state and territory, and national incident notification and reporting obligations. Include details about who in your organisation is responsible for incident notification and reporting to external entities.

You could include this in a table, for example:

Incident type/ threshold	**Organisation/ agency to receive notification or report**	**Contact details for the notifying organisation/agency**	**Key notifying/reporting requirements and link to organisation/agency information** (e.g. incident type, severity, deadlines)	**Personnel responsible** (e.g. CIRP role title)
e.g. Ransomware	Australian Cyber Security Centre (ACSC)	P: 1300 CYBER1 E: asd.assist@defence.gov.au	Refer to https://www.cyber.gov.au/acsc/report	
e.g. Data breach	Office of the Australian Information Commissioner (OAIC)	See contact details at https://www.oaic.gov.au/about-us/contact-us/	Refer to https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach/	

10.1. Legal and Regulatory Requirements

Include details about the legal and regulatory obligations relevant to your organisation, such as reporting requirements.

Work with your organisation's compliance/legal team to ensure the cyber incident response plan meets all relevant legal/regulatory requirements. Different incidents may require different or multiple legal and regulatory requirements.

The CIRP could include a process chart of when to report incidents to relevant organisations and regulators.

Include details about additional legal or privacy considerations that may impact your response (e.g. contractual obligations).

10.2. Insurance

Include relevant details about your organisation's insurance policy for cyber incidents.

INCIDENT RESPONSE PROCESS

11. Detection, Investigation, Analysis and Activation

Include your organisation's decision making framework for activating the CIRP.

Refer to your separate Standard Operating Procedures for incident detection, investigation and analysis. This may include how you become aware of an event or incident and your immediate actions in response.

Incidents could be detected in several ways, including, but not limited to:

- Self-detected incidents (e.g. Intrusion Detection and Prevention systems)
- Notifications received from service providers or vendors
- Notifications received from trusted third parties such as the ACSC.

11.1. Incident Classification

Include your organisation's framework and decision making process for classifying a cyber incident. This can assist with prioritising resources. Classification factors could include:

- Effects of the incident (confidentiality, integrity and availability of information and systems)

- Stakeholders affected (internal and external)
- Incident type
- Impact on the business and community

For example:

Incident Classification	Descriptions
Critical	Over 80% of staff (or several critical staff/teams) unable to work Critical systems offline High risk to/definite breach of sensitive client or personal data Financial impact >$insert Severe reputational damage – likely to impact business long term
High	50% of staff unable to work Non critical systems affected Risk of breach of personal or sensitive data Financial impact >$insert Potential serious reputational damage
Medium	20% of staff unable to work Small number of non-critical systems affected Possible breach of small amounts of non-sensitive data Financial impact >$insert Low risk to reputation
Low	<10% of non-critical staff affected temporarily (short term) Minimal, if any, impact One or two non-sensitive/non-critical machines affected No breach of data Negligible risk to reputation

For information about the ACSC Incident Categorisation Framework see Appendix K.

11.2. Cyber Incident Response Team (CIRT) Activation

Include your organisation's decision making framework for activating the CIRT. (Note: some smaller incidents may be manageable without activation of the CIRT). This could align with the Incident Classification framework.

11.2.1 Logistics and Communications

Include core logistical and communications protocols, mechanisms to support incident response. For example:

- Operations Room/Security Operations Centre (SOC) location and setup
- Kit required for offsite incident response
- Communications technologies such as phone/teleconference/online dial-in details, out-of-bands communications (e.g. Slack or other similar applications).

11.3. Investigation Questions

To guide your incident response efforts and understanding of the scope and impact of the incident, develop a list of investigation questions. Not all questions may be answerable with the data available and questions may change as your investigation progresses.

Possible investigation questions include:

- What was the initial intrusion vector?
- What post-exploitation activity occurred? Have accounts been compromised? What level of privilege?
- Is lateral movement suspected or known? Where has the actor laterally moved to and how?
- How is the actor maintaining command and control?
- Does the actor have persistence on the network or device?
- Has data been accessed or exfiltrated and, if so, what kind of data?

11.4. Escalation and De-escalation

Include the escalation and de-escalation triggers and/or thresholds, and decision making authorities. You could include this in a table, for example:

Incident Classification	Action	Triggers and/or thresholds for escalation and de-escalation	Minimum level authority
Critical	De-escalate to High		
High	Escalate to Critical		
	De-escalate to Medium		
Medium	Escalate to High		
	De-escalate to Low		
Low	Escalate to Medium		

12. Containment, Evidence Collection and Remediation

12.1. Containment

Refer to your organisation's separate detailed SOPs about containing the incident according to the incident type.

Containment actions are implemented in order to minimise the damage, prevent the incident from spreading or escalating, and prevent the attacker from destroying evidence of their attack.

When planning containment actions, consider:

- Any additional impacts there could be to systems/services

- Time and resources required to contain the incident
- Effectiveness of the containment solution (e.g. partial vs full containment)
- Duration that the solution will remain in place (e.g. temporary vs permanent solution)

12.2. Documentation

Include your organisations process for documenting the incident, responsible personnel, recipients and timeframes. Refer to Appendix D for a Situation Report template and Appendix E for Incident Log template.

Situation reports may contain the following information:

- Incident date and time
- Status of the incident
- Incident type and classification
- Scope and Impact
- Severity
- External assistance required
- Actions taken to resolve the incident
- Contact details for incident manager and key CIRT personnel
- Date and time of the next update

12.3. Evidence Collection and Preservation

Include your organisation's processes for collecting, preserving, handling and storing evidence, responsible personnel, recipients and timeframes. As this can be complex you may need to seek advice from digital forensic professionals, legal or law enforcement.

When gathering evidence, maintain a detailed log that clearly documents how all evidence has been collected. This should include who collected or handled the evidence, the time and date (including time zone) evidence was collected and handled, and the details of each item collecting (including the location, serial number, model number, hostname, media access control (MAC) address, IP address and hash values). See Appendix F for a template.

Examples of commonly collected evidence include:

- Hard drive images and raw images
- RAM images
- IP addresses
- Network packet captures and flows
- Network diagrams
- Log files
- Configuration files
- Databases
- IR/investigation notes
- Screenshots
- Social media posts
- CCTV, video and audio recordings
- Documents detailing the monetary cost of remediation or loss of business activity

12.4. Remediation Action Plan

Include your organisation's process for developing and implementing a Remediation Action Plan to eradicate and resolve the incident, following successful containment and evidence collection. See Appendix G for a template.

When developing the Remediation Action Plan, consider:

- What actions are required to eradicate/resolve the incident?
- What resources are required to resolve the incident (if not already included in the CIRT)?
    - Are there additional external resources you may require?
- Who is responsible for remediation actions?

- What systems/services should be prioritised?
- What systems/services will be affected during the remediation process? How will these systems be affected?
- What is the expected resolution time?

13. Recovery

Include your organisation's process for developing, authorising and executing an agreed recovery plan.

The recovery plan should detail the approach to recovering IT and/or OT networks, systems and applications once containment and eradication is complete.

When developing the Recovery Plan, consider:

- How systems will be restored to normal operation and expected timeframes?
- How systems will be monitored to ensure they are no longer compromised and are functioning as expected?
- How identified vulnerabilities will be managed to prevent similar incidents?

13.1. Stand Down

Include your organisation's process, including decision making for standing down the CIRT and SEMT.

Include your process for completing an incident report, including recipients and timeframes. Consider creating an incident report template as an appendix to the CIRP.

14. Learn and Improve

Include your organisation's approach to learn from the incident and improve.

14.1. Post Incident Review

A Post Incident Review (PIR) is a detailed review conducted after an organisation has experienced a cyber security incident. It can include a hot debrief which is held immediately after an organisation has recovered its networks and systems from a cyber security incident and a formal debrief held after the incident report has been completed, such as within two weeks.

Key questions to consider in your PIR:

- What were the root causes of the incident and any incident response issues?
- Could the incident have been prevented? How?
- What worked well in the response to the incident?
- How can our response be improved for future incidents?

Refer to Appendix H for more detailed questions to consider in your PIR.

Recommendations that arise from the review can be documented in a corresponding Action Register. Refer to Appendix I for an Action Register template.

14.1.1 PPOSTTE Model

The PPOSTTE model can assist to reflect on key elements of the incident response.

People	Roles, responsibilities, accountabilities, skills
Process	Plans, policies, procedures, protocols, processes, templates, arrangements
Organisation	Structures, culture, jurisdictional arrangements
Support	Infrastructure, facilities, maintenance
Technology	Equipment, systems, standards, security, inter-operability
Training	Qualifications/skill levels, identification of required courses
***Exercise Management** *This only applies to exercises*	Exercise development, structure, management, conduct

14.2. Update and Test Cyber Incident Response Plan

The PIR may result in changes to your CIRP, Playbooks and Templates. Changes should be communicated to the relevant personnel.

Significant changes may require the CIRP and Playbooks to be tested. Regular testing is important to ensure these documents remain current and are familiar to the relevant personnel. Testing methods could include discussion or functional exercises.

14.3. Training

Include your organisation's training activities to support personnel named in the CIRP to perform their roles.

The PIR may identify training needs for staff involved in incident response or cyber security awareness training for all staff.

Consider how your organisation will support your staff through training activities.

APPENDICES

Appendix A – Terminology and Definitions

Use of consistent and pre-defined terminology to describe incidents and their effects can be helpful during a response. In your CIRP, include commonly used terms used in your organisation. ACSC defines cyber threats, events, alerts and incidents as follows:

Cyber threat

A cyber threat is any circumstance or event with the potential to harm systems or information. Other threats are listed on cyber.gov.au. Organisations can include a list of cyber threats of concern. The ACSC Annual Cyber Threat Report (2021) outlines the following threat environment and key cyber security trends:

- COVID-19 themed malicious activity including phishing emails and scams
- Ransomware
- Exploitation of security vulnerabilities
- Software supply chain compromise
- Business Email Compromise
- Cybercrime

Cyber security event

A cyber security event is an occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security.

A cyber security event has the potential to become, but is not confirmed to be, a cyber incident.

Examples of cyber security events include (but are not limited to):

- A user has disabled the antivirus on their computer
- A user has deleted or modified system files
- A user restarted a server
- Unauthorised access to a server or system.

Cyber security alert

A cyber security alert is a notification generated in response to a deviation from normal behaviour. Cyber security alerts are used to highlight cyber security events.

Cyber incident

A cyber incident is an unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations. A cyber incident requires corrective action.

Examples of cyber security incidents include (but are not limited to):

- Denial-of-service attacks (DoS)
- Unauthorised access or attempts to access a system
- Compromise of sensitive information
- Virus or malware outbreak (including ransomware).

Appendix B – Cyber Incident Response Readiness Checklist

This checklist is to aide your organisation's initial assessment of its readiness to respond to a cyber security incident. This checklist is not an exhaustive list of all readiness activities.

Organisations can tailor the checklist to include additional readiness activities relevant to their organisation.

Preparation	
☐	Your organisation has a cyber security policy or strategy that outlines your organisation's approach to prevention, preparedness, detection, response, recovery, review and improvement. ○ For example, does your organisation have a position on, for example, paying ransom, reporting incidents to government, publicly acknowledging cyber incidents, sharing information about incidents with trusted industry and government partners?
☐	A Cyber Incident Response Plan has been developed, which: ○ Aligns with your organisation's operating environment and other processes, including emergency management and business continuity processes. ○ Has been reviewed or tested in an exercise to ensure it remains current and responsible personnel are aware of their roles, responsibilities and processes. ○ Templates have been prepared, for example Situation Reports.
☐	Staff involved in managing an incident have received incident response training.
☐	Up-to-date hard copy versions of the Cyber Incident Response Plan and playbooks are stored in a secure location (in case of electronic or hardware failure) and are accessible to authorised staff members.
☐	Specific playbooks to supplement the Cyber Incident Response Plan have been developed, that define step-by-step guidance for response actions to common incidents, and roles and responsibilities.
☐	A Cyber Incident Response Team (CIRT) and a Senior Executive Management Team (SEMT) – or equivalents - have been formed to manage the response, with approved authorities.
☐	All relevant IT and OT Standard Operating Procedures (SOPs) are documented and have been reviewed or tested in an exercise to ensure they remain current and responsible personnel are aware of their roles, responsibilities and processes.
☐	Arrangements for service providers, including cloud and software as a service, to provide and retain logs have been established and tested to ensure these include useful data and can be provided in a timely manner.
☐	Log retention for critical systems have been configured adequately and tested to confirm that they capture useful data. Refer to the ACSC publications including Windows Event Logging and Forwarding for specific guidance.
☐	Your organisation has internal or third party arrangements and capabilities to detect and analyse incidents. If these capabilities are outsourced, your organisation has an active service agreement/contract).
☐	Critical assets (data, applications and systems) have been identified and documented.

☐	Standard Operating Procedures (SOPs) have been developed, and roles and responsibilities assigned for use of facilities and communications technologies in response to cyber incidents, and these resources are confirmed as available. This includes for alternative/back-up ICT-based channels.
☐	Incident logging/records and tracking technologies used to manage a response are confirmed as available and have been tested.
☐	Role cards have been developed for each person involved in the CIRT and the SEMT. Individual actions will depend on the type and severity of the incident. Example role card is available at Appendix J.
☐	Your organisation has internal or third party arrangements and capabilities to monitor threats. Situational awareness information is collected from internal and external data sources, including: ○ Local system and network traffic and activity logs ○ News feeds concerning ongoing political, social, or economic activities that might impact incident activity ○ External feeds on incident trends, new attack vectors, current attack indicators and new mitigation strategies and technologies.
Detection, Investigation, Analysis and Activation	
Standard Operating Procedures (SOPs) have been developed, and roles and responsibilities assigned for:	
☐	Detection mechanisms which can be used to identify potential information security incidents, such as scanning, senses and logging mechanisms. These mechanisms require monitoring processes to identify unusual or suspicious activity, for example behaviour and logging, commensurate with the impact of an incident. Common monitoring techniques include: a) network and user profiling that establishes a baseline of normal activity which, when combined with logging and alerting mechanisms, can enable detection of anomalous activity; b) scanning for unauthorised hardware, software and changes to configurations; c) sensors that provide an alert when a measure breaches a defined threshold(s) (e.g. device, server and network activity); d) logging and alerting of access to sensitive data or unsuccessful logon attempts to identify potential unauthorised access; and e) users with privileged access accounts subject to a greater level of monitoring in light of the heightened risks involved.[4]
☐	Incident detection, including self-detected incidents, notifications received from service providers or vendors, and notifications received from trusted third parties (e.g. ACSC).
☐	Incident analysis, including how incidents are to be categorised, classified and prioritised, and controls related to how data is stored and transmitted (i.e. if out-of-band transmission is required).
☐	Activating a Cyber Incident Response Team (CIRT) to manage critical incidents, with roles and responsibilities assigned.

[4] APRA Prudential Practice Guide CPG 234 Information Security.

☐	Activating a Senior Executive Management Team (SEMT) to manage critical incidents, with roles and responsibilities assigned.
Containment, Evidence Collection and Remediation	
☐	Standard Operating Procedures (SOPs), playbooks and templates, have been developed, and roles and responsibilities assigned for containment, evidence collection and remediation. These can be included as appendices to the Cyber Incident Response Plan.
☐	A secure location is available for storing data captured during an incident, which could be used as evidence of the incident and the adversary's tradecraft, and ready to be provided to third-party stakeholders if needed.
Communications	
☐	Policy, plans, Standard Operating Procedures (SOPs) and templates have been developed to support communicating with: ○ Internal stakeholders (e.g. Board, staff) ○ External stakeholders (e.g. stakeholders to assist with the response and stakeholders with an interest in the response)
☐	Policy, plans, Standard Operating Procedures (SOPs) and templates for media and communications professionals have been developed, and roles and responsibilities assigned, to support public and media messaging.
☐	You organisation has assigned a public and media spokesperson, who is supported by subject matter experts.
☐	Staff have been trained to implement the communications processes and execute their roles and responsibilities.
☐	Staff who are not involved in managing incidents are cognisant of your organisation's policy and processes and their responsibilities when an incident occurs (e.g. exercising discretion, using approved talking points, referring enquiries to the designated officer).
Incident Notification and Reporting	
☐	Processes and contact details are documented to support the organisation to meet its legal and regulatory requirements on cyber incident notification, reporting and response, with roles and responsibilities within your organisation are assigned. This includes the processes for obtaining authority to release and share information.
☐	Processes are documented for insurance requirements.
Post Incident Review	
☐	A process is documented to conduct Post Incident Reviews (PIR) following conclusion of an incident and PIR reports with recommendations are submitted to management for endorsement.
☐	A process is documented to ensure actions following incidents and/or exercises are tracked and completed (e.g. Action Register).

Appendix C – ACSC Incident Triage Questions

Where applicable, personnel reporting cyber security incidents to the ACSC on behalf of their organisation should try to have information available to answer the following questions:

- Who is reporting the incident? (include their position e.g. CISO, ITSA, SOC Manager etc.)
- Who/what is the affected organisation/entity?
- What type of incident is being reported? (e.g. ransomware, denial of service, data exposure, malware)
- Is the incident still active?
- When was the incident first identified?
- Are you reporting for ACSC awareness or is ACSC assistance required?
    - If ACSC assistance is required, what assistance is needed?
- What type of system or network has been affected?
    - Information Technology (IT)
        - Corporate systems/networks, databases, servers, VOIP systems.
    - Operational Technology (OT)
        - SCADA, Remote sensors, BMS/BAS, logic controllers.
- What was observed (the sequence of events)? E.g. was lateral movement observed?
    - Date/Time
    - Effect/Event
- Who or what identified the problem?
- Has a data breach occurred?
    - What type of information was exposed?
        - What impact will this have on the organisation?
        - What impact (if any) will the breach have on public safety or services?
    - What volume of records/data was exposed?
    - Was it a misconfiguration/error, or was a malicious exfiltration or theft of data identified?
    - Has it been reported to the Office of the Australian Information Commissioner (OAIC)?
        - If not, organisations need to consider if mandatory reporting obligations apply under the Notifiable Data Breach (NDB) scheme
- What actions have been taken to rectify the issue?
    - Does the organisation/entity have internal or external IT and/or cyber security incident response providers?
    - Are services/business as usual operations interrupted?
        - If so, how long do they expect before they are back at normal operating capability?
- Will you be communicating publicly about the incident and engaging with media? ;
    - If so, please notify the ACSC beforehand if you will be referencing the ACSC.

Appendix D – Situation Report Template

Date of entry:	**Time of entry:**	**Author:**
Date and Time incident detected		
Current Status	e.g. New | In Progress | Resolved	
Incident Type		
Incident Classification		
Scope – list the affected networks, systems and/or applications; highlight any change to scope since the previous log		
Impact – list the affected stakeholder(s); highlight any change in impact since the previous log entry		
Severity – outline the impact of the incident on your organisation(s) and public safety or services; highlight any change to severity since the previous log entry		
Notifications Actioned/Pending		
Assistance required – what assistance do we require from other organisations? (e.g. ACSC, law enforcement)		
Actions taken to resolve incident		
Additional notes		
Contact details for incident manager and others if required		
Date and Time of next update		

Appendix E – Incident Log Template

Date and Time	**Notes** (relevant facts, decisions, rationale)

Appendix F – Evidence Register Template

Date, Time and Location of collection	**Collected by** (name, title, contact and phone number)	**Item Details** (quantity, serial number, model number, hostname, media access control (MAC) address, IP addresses and hash values)	**Storage location and label number**	**Access**

Appendix G – Remediation Action Plan Template

Date and Time	**Category** (Contain, Eradicate, Recover)	**Action**	**Action Owner**	**Status** (Unallocated, In Progress, Closed)

Appendix H – Post Incident Review Guide Template

Incident Summary

Incident name	
Date of incident	*dd/mm/yy*
Incident Priority	*Low/Medium/High* *Established from the impact and/or risk to the business*
Time incident occurred	
Time incident was resolved	
Incident type	*Malware, etc.*
Personnel involved	*Names of the individuals involved in resolving the incident and their function(s), including any service providers*
Incident impact	*What impact did the incident have? I.e. loss of systems*
Brief summary	*What happened?*

Incident Analysis

The Incident Analysis is broken into the following categories:

- **Incident timeline -** Summary of what happened and when. Provides high level areas for improvement.
- **Protection** - Identifies the protection mechanisms that were in place at the time of the incident and their effectiveness. Establishes how to improve the protection of our systems and networks.
- **Detection -** Establishes how to reduce the time to identify an incident is occurring. Addresses what detection mechanisms were in place, and how those mechanisms can be improved.
- **Response -** Identifies improvements for the incident response.
- **Recovery -** Addresses improvements for incident recovery (i.e. how to recover from an incident faster).

INCIDENT TIMELINE	
Date and time of detection	
When was the incident acknowledged?	*When did your organisation identify that an incident was occurring?*
Date and time of incident response	
Date and time of incident recovery	

Who discovered the incident first and how?	*Or who was alerted to it first? How did the discovery or alert happen?*
Was the incident reported externally? If yes, when?	*For example, did your organisation report it to the ACSC?*
Who supported resolving the incident? When did they provide support?	*List the names of personnel involved in resolving the incident, and the time (and date if not all on the same day) they joined in.*
What activities were conducted to resolve the incident? When were they conducted and what was their impact?	*It is easier to do this in a list, for example:* *Time > Task > Impact*
PROPOSED ACTIONS	*Detail any resulting actions that can be incorporated into the Action Register.* *Brief description of action > Proposed Action Officer*

PROTECTION	
What <u>controls</u> were in place that were expected to stop an incident similar to this?	*I.e. systems, networks, etc.*
How effective were those <u>controls</u>?	*Did they work? Why/why not?* *How could they be improved?*
Are there other <u>controls</u> considered better for protecting against a similar incident?	*What are they?*
What <u>business processes</u> were in place to prevent this type of incident from occurring?	*I.e. Your organisation's policies and procedures.*
How effective were those <u>business processes</u>?	*Did they work? Why/why not?* *How could they be improved?*
Any other findings and/or suggestions for improvement?	***See the PPOSTTE model for guidance*
PROPOSED ACTIONS	*Detail any resulting actions that can be incorporated into the Action Register.* *Brief description of action > Proposed Action Officer*

INCIDENT DETECTION	
How was the incident detected?	*How did you know the incident was happening?*
What <u>controls</u> were in place to detect the incident?	

Were those controls effective?	*Did they work? Why/why not?*
What business processes were in place to detect the incident?	
Were those business processes effective?	*Did they work? Why/why not?*
Are there any ways to improve the 'time-to-detection'?	*How could your organisation reduce that time?*
Are there any indicators that can be used to detect similar incidents in the future?	
Are there any additional tools or resources that are required in the future to detect similar incidents?	*Is there anything (from a detection perspective) that will help mitigate future incidents?* *Technology? Human resources with specific skills? Etc.*
Any other findings and/or suggestions for improvement?	*What activities worked well? What activities did not work so well? What could be changed with hindsight?* ***Also see the PPOSTTE model for guidance*
PROPOSED ACTIONS	*Detail any resulting actions that can be incorporated into the Action Register.* *Brief description of action > Proposed Action Officer*

INCIDENT RESPONSE	
What was the cause of the incident?	
How was the incident resolved?	*What needed to happen for the issue to be resolved?*
What obstacles were faced when responding to the incident?	
Were any business policies and/or procedures used in responding to the incident?	*For example, does your organisation have an Incident Response Plan, and was this followed?*
Were those business policies and/or procedures effective?	*Did they work? Why/why not?*
What delays and obstacles were experienced when responding?	
Were there any escalation points?	*Were there any escalation points that the incident went through?*
If there were escalation points, did they hamper the response OR were they at the appropriate level?	*For example, having to escalate to a Chief Operating Officer (COO) to take action on an ongoing incident had severe timeline impacts on responding to an active incident.*
How well did the information sharing and communications work within your organisation?	*What worked well/what did not work well. How could it be improved?* *Was there any information that was needed sooner?*

	How did your organisation communicate within the IR team, across jurisdictions, across time zones, legal teams, external comms teams, etc.?
Were there any media enquiries received during the incident?	*If yes, WHAT was the media, and how did your organisation respond?*
Was media produced during the incident?	*If yes, WHAT was the media, and how did your organisation respond?*
Was the customer notified during the incident?	*Why/why not? When? How?*
Were trained staff available to respond?	*Are there any staff knowledge and/or skills gaps? What are they?* *Were there enough resources available to respond?*
Any other findings and/or suggestions for improvement?	***See the PPOSTTE model for guidance*
PROPOSED ACTIONS	*Detail any resulting actions that can be incorporated into the Action Register.* *Brief description of action > Proposed Action Officer*

INCIDENT RECOVERY	
How long did it take for all systems and networks to recover?	
How could this time be improved?	*For example, how could the recovery time be reduced?*
Are there any obligations to report externally about the incident?	
Were there any media enquiries after the incident?	
Were staff and/or customers notified of the incident?	*Why/why not?* *How was the notification completed? Was it effective? How could it be improved?*
Any other findings and/or suggestions for improvement?	***See the PPOSTTE model for guidance*
PROPOSED ACTIONS	*Detail any resulting actions that can be incorporated into the Action Register.* *Brief description of action > Proposed Action Officer*

Appendix I – Action Register Template

ID	Action	Action Officer	Date expected to complete	Status	Updates	Comments
A01	Describe the action in detail	Name of the person who will be leading the action	Date the action is expected to be completed	Complete In progress Not yet started	Insert date, and any updates to progressing the action You can also detail any blockers here	Any relevant information relating to closing out the action
A02						
A03						
A04						
A05						
A06						
A07						
A08						
A09						
A10						

Appendix J – Role Cards

Example of a role card:

ROLE CARD – CYBER INCIDENT RESPONSE

INCIDENT MANAGER

Reports to SEMT Chair

RESPONSIBILITIES

- Activate the CIRP
- Coordinate operations room setup
- Manage a team of incident responders including preparing for, and tracking, daily investigation tasks
- Provide administrative and logistical support for incident responders
- Manage the passage of relevant operational information to the SEMT

ROLE CARD – CYBER INCIDENT RESPONSE

KEY CONTACTS

Virtual Meeting Room:
XXXX

Backup conference line:
XXXX

Media:
XXXX

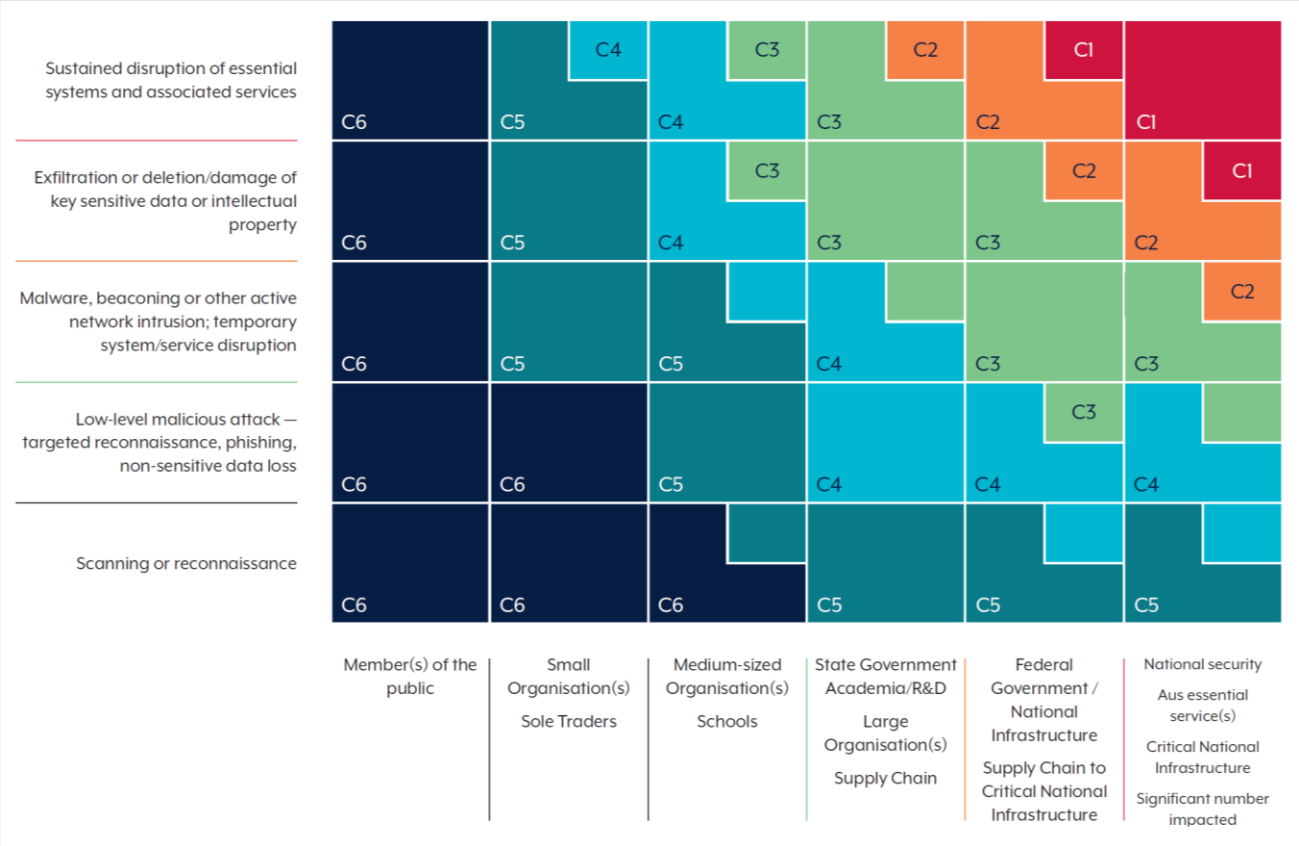
Security:
XXXX

Legal:
XXXX

Appendix K – ACSC Incident Categorisation Framework

ACSC categorises cyber incidents by severity using a framework that considers the:

- Impact (i.e. the known or likely effects, and/or importance of the affected services and data)
- Victim (i.e. significance and/or number of victims)



The severity of the cyber incident informs the type and nature of incident response and crisis management arrangements that are activated. Depending on the severity of the incident, the ACSC has a suite of capabilities that it may deploy to support the affected parties. However, ACSC determines which capabilities are appropriate and available given competing priorities. Organisations must not rely on the ACSC for their own ability to respond to cyber incidents in an appropriate and timely manner.