Cyber Security Incident Management Plan

For limited, major or critical non-emergency cyber security incidents

October 2024

VICTORIA State Government | Government Services

Publication information

The State Crisis and Resilience Council approved this Cyber Security Incident Management Plan (CSIMP, or 'the Plan') on 10 October 2024.

The Plan has been prepared by the Department of Government Services (DGS) as the Victoria's portfolio department for cyber security.

Authorised and published by the Victorian Government, Melbourne October 2024

© Copyright State of Victoria 2024

You are free to re-use this work under a Creative Commons Attribution 4.0 licence, provided you credit the State of Victoria (Department of Government Services) as author, indicate if changes were made and comply with the other licence terms. The licence does not apply to any images, photographs or branding, including government logos.

Licence URL:	creativecommons.org/licenses/by/4.0/
Attribution:	© Copyright State of Victoria 2024
Acknowledgement:	Cover page photo by © Green Creator – stock.adobe.com Page ii photo by Markus Spiske – Unsplash – unsplash.com Page 6 photo by Adam Nowakowski – Unsplash – unsplash.com Back cover page photo by © aniaostudio – istockphoto.com

This document is available in accessible format at www.vic.gov.au/prepare-cyber-incident.

Contents

Page	Section	
1	**1**	**Summary**
1	1.1	Summary of the plan
1	1.2	Summary of incident phases
3	**2**	**Defining and categorising cyber security incidents**
3	2.1	Defining 'cyber security incident'
3	2.2	Categorising a cyber security incident
7	**3**	**Introduction to arrangements**
7	3.1	Our collective cyber security vision
7	3.2	Shared responsibility
8	3.3	About this plan
10	3.4	Wider state and federal government arrangements
12	3.5	Audience
14	3.6	State significant risk
14	3.7	Core expectations
15	**4**	**Cyber security incident mitigation**
15	4.1	Improving cyber security maturity
16	4.2	Threat intelligence
18	4.3	Community and industry awareness and engagement
19	**5**	**Cyber security incident preparedness (identify, protect and detect)**
19	5.1	Identify and protect from cyber security risk
20	5.2	Maintain and exercise plans and arrangements
21	5.3	Detection
23	**6**	**Cyber security incident response**
23	6.1	Analysis
24	6.2	Notification and classification
28	6.3	Technical response, including containment and eradication
29	6.4	Control and coordination
31	6.5	Consequence management
34	6.6	WoVG Control Team or Consequence Coordination Team
36	6.7	Control or coordination centre
36	6.8	Media and public communication
38	6.9	Managing concurrent cyber security incidents
38	6.10	Controlling Victoria's consequences of a national cyber incident or emergency
41	**7**	**Cyber security incident recovery**
41	7.1	Summary
42	7.2	Social recovery
42	7.3	Economic recovery
42	7.4	Built recovery
43	7.5	Natural recovery
43	7.6	Aboriginal culture and healing
43	7.7	Roles and responsibilities
44	7.8	Closing out an incident
45	**8**	**Lessons and evaluation**
46	**9**	**Appendices**
46		Appendix A: Acronyms
49		Appendix B: Common sources of cyber security compromise or consequence
50		Appendix C: Comparison of Whole of Victorian Government cyber security incident categories with Business Impact Levels
51		Appendix D: State Emergency Management Priorities
52		Appendix E: Sector Resilience Networks
53		Appendix F: Frameworks for cyber security maturity
56		Appendix G: Summary of threat intelligence products
57		Appendix H: Contact details of key stakeholder agencies
58		Appendix I: Summary of Australasian Inter-Service Incident Management System functions

Acknowledgment of Country

DGS acknowledges Aboriginal and Torres Strait Islander people as the Traditional Custodians of the land.

DGS also acknowledges and pays respect to Elders, past and present. DGS is committed to working with Aboriginal and Torres Strait Islander communities to achieve a shared vision of safer and more resilient communities.

Acronyms

Acronyms can be used for various terms in this Plan. These acronyms are defined in **Appendix A**.

Version

This is the second version of the Plan. The Department of Premier and Cabinet (DPC) prepared the original when it managed the cyber security portfolio. DPC transferred the Victorian Government's cyber security portfolio to DGS when DGS was established on 1 January 2023.

This Plan may be read together with the State Emergency Management Plan Cyber Security Sub-Plan (the Sub-Plan) as they cover content relevant to both incidents and emergencies (for example, mitigation activities). Where there is crossover, the Sub-Plan takes precedence over this Plan.

Plan activation

This plan is current at the time of publication. It remains in effect until it is modified, superseded or withdrawn.

The arrangements in this plan are ongoing and do not require activation.

1 Summary

1.1 Summary of the plan

Cyber security incidents are a serious threat to Victorians. They happen more often and are more complex than ever before.

The Victorian Government needs to plan to protect Victorians. Planning should address what happens before, during and after cyber security incidents.

This document is the Cyber Security Incident Management Plan (CSIMP, or 'this Plan'). It supports departments and government agencies through all stages of an incident.

Its scope is the Whole of Victorian Government (WoVG).

It covers 3 types of incidents which need a WoVG response. These include limited, major and critical cyber security incidents.

A separate plan covers cyber security emergencies. That is the State Emergency Management Plan Cyber Security Sub-Plan ('the Sub-Plan').

The CSIMP outlines the roles for each department and government agency.

Each department and government agency is in charge of how they respond to an incident. They each have their own internal plan. The CSIMP works alongside these internal plans.

1.2 Summary of incident phases

1.2.1 Mitigation

Mitigation means actions which stop or reduce the impact of incidents. Mitigation is important at all stages of an incident.

In this Plan, mitigation involves:

- improving systems and services
- collecting, analysing and sharing information about potential threats
- providing the right advice to industry and the community at the right time.

1.2.2 Preparedness

Preparedness means actions taken before an incident occurs. This allows a department or government agency to be ready for an incident and its potential impacts.

In this Plan, preparedness involves:

- identifying potential weaknesses in systems
- keeping internal plans up to date
- monitoring for potential compromises.

1.2.3 Response

Response means actions taken during an incident to address it and its impacts.

In this Plan, response involves:

- understanding the incident as it is happening
- classifying the incident based on its current and expected impacts
- giving correct information to the right people as soon as possible
- containing and removing the incident's cause
- directing response activities across departments and government agencies
- providing centralised strategic advice across WoVG from the control team
- activating a location as the control centre
- managing Victoria's role during a national cyber security incident
- prioritising resources when there is more than one incident at a time
- bringing in various resources, as required
- sharing information and warnings through the media
- evaluating and managing consequences which may arise after an incident
- providing relief during and after an incident.

1.2.4 Recovery

Recovery means actions which address the impacts of an incident after it has occurred.

In this Plan, recovery involves:

- returning systems and processes to proper function
- deciding how to move forward once an incident no longer needs a WoVG response.

1.2.5 Lessons and evaluation

Following an incident, it is important to identify what worked well and what needs improvement.

2 Defining and categorising cyber security incidents

2.1 Defining 'cyber security incident'

The Cyber Incident Management Arrangements for Australian Governments (CIMA) define a cyber security incident as "a single or series of unwanted or unexpected event(s) that impact the confidentiality, integrity or availability of a network or system or the information that it stores, processes or communicates".

Appendix B expands on common sources of cyber security compromise or consequence. These include:

- ransomware
- malware infections
- denial of service (DoS) and distributed denial of service (DDoS) attacks
- phishing and social engineering
- a data breach.

2.2 Categorising a cyber security incident

Table 1 shows different cyber security events, incidents and emergencies and how they are categorised.

A summary of notification requirements for each level of severity is included here, with the full notification requirements for limited, major and critical incidents included in the 'Notification' section.

These WoVG cyber security categories are prepared as a comparable state level equivalent to the Office of the Victorian Information Commissioner (OVIC) entity-level Business Impact Levels (see **Appendix C**).

Table continues next page.

TABLE 1: WoVG cyber security categories

Severity (low to high)	WoVG category (incident or threat)	Common traits	Internal plan	WoVG plan	Initial notification requirements
1	**Event**	This is a suspected or unconfirmed cyber security compromise that causes no impact to systems, services or information (such as, malicious scanning activity). Alternatively, it can mean a confirmed cyber security event or threat that does not impact any department or government agency.	Department or government agency's internal cyber security incident response plan, enacted internally	No WoVG plan	Notification to CIRS is not required.
2	**Minor**	This is a successful cyber security compromise. The compromise has potential to cause or is causing minor impact to services, information, assets, reputation or relationships. This involves: → a response using routine internal procedures, within a department or government agency's normal response capability and capacity → an assumption that the incident will not spread to another department or government agency.			To inform intelligence, notification is required to DGS' Cyber Incident Response Service (CIRS) **within 72 hours** via the Whole of Victorian Government Cyber Security Portal
3	**Limited**	This is a successful cyber security compromise. The compromise has potential to cause or is causing limited impact to services, information, assets, government reputation, relationships and/or the community. This involves at least one of the following consequences: → direct or indirect impacts to a department or government agency's ability to ensure the confidentiality, integrity or availability of its systems, services or data → disruption to activities requiring reprioritisation of activities or resourcing to meet expected levels of service → impacts to critical business operations and other systems → potential to spread to another department or government agency → a response required at the state level, involving: → monitoring and analysis → sharing indicators of compromise, mitigation advice and options → a need to coordinate a WoVG response in support of a Commonwealth-led incident. Alternatively, it can mean a cyber security threat where there is: → a major scheduled event which may be an attractive target for a cyber attack → information or intelligence that identifies a cyber security threat that warrants increased monitoring and analysis.	Department or government agency's internal cyber security incident response plan, enacted internally	**This Plan** (takes precedence), enacted by the Manager of CIRS or Victorian Government Chief Information Security Officer (CISO)	Notification is required to: → CIRS, **within 72 hours**, via the Whole of Victorian Government Cyber Security Portal or 1300 278 842 (if outside of business hours) → other stakeholders, as per the notifications section

4	**Major**	This is a successful cyber security compromise. This compromise has potential to cause or is causing major impact to services, information, assets, government reputation, relationships and/or the community.
		This involves at least one of the following consequences:
		→ ineffectiveness of a department or government agency's ability to ensure the confidentiality, integrity or availability of its systems, services or data
		→ disruption to activities requiring reprioritisation of activities or resourcing to meet expected levels of service
		→ activation of business continuity plans
		→ direct or indirect major impacts to more than one department or government agency
		→ a large-scale data breach
		→ media interest generated by public concern
		→ an immediate response required at the state level, involving strategic coordination and engagement to:
		  → advise stakeholders, detailing the threat and potential or actual impacts
		  → share indicators of compromise, mitigation advice and options
		  → develop and/or share response capability across jurisdictions
		  → engage media, government and Victorians
		→ consideration to share and deploy technical resources across departments and request Australian Cyber Security Centre (ACSC) assistance
		→ a need to coordinate a WoVG response in support of a Commonwealth-led incident or crisis.
		Alternatively, this can mean a cyber security threat where information or intelligence warrants immediate monitoring and analysis (e.g. increased cyber threat activity, which may extend across Victoria or nationally).
			Department or government agency's internal cyber security incident response plan, enacted internally	**This Plan** (takes precedence), enacted by the Manager of CIRS or Victorian Government Chief Information Security Officer (CISO)	Notification is required to:
					→ CIRS, **within 12 hours**, via the Whole of Victorian Government Cyber Security Portal or 1300 278 842 (if outside of business hours)
					→ other stakeholders, as per the notifications section

5	**Critical**	This is a successful cyber security compromise. This compromise has potential to cause or is causing significant impact to services, sensitive information, assets, government reputation, relationships and/or the community.
		This involves at least one of the following consequences:
		→ sustained disruption to a department or government agency's ability to ensure the confidentiality, integrity or availability of its systems, services or data, directly or indirectly
		→ malicious cyber activity where the cause and potential extent is uncertain
		→ links across multiple departments, government agencies or Australian jurisdictions requiring a coordinated WoVG response
		→ an immediate response required at the state level, involving strategic coordination and engagement to:
		  → advise stakeholders, detailing the threat and potential or actual impacts
		  → share indicators of compromise, mitigation advice and options
		  → develop and/or share response capability across jurisdictions
		  → engage media, government and Victorians
		  → consider sharing and deploying technical resources across departments and government agencies, and request Commonwealth assistance.			

6	**Emergency**	This is a serious or exceptional compromise of cyber security. This compromise has potential to cause or is causing at least one of the following consequences: → death or serious injury → extensive damage to property, infrastructure or the environment → widespread disruption, damage or destruction of critical infrastructure → disruption to emergency services requiring reprioritisation to meet expected levels of service → significant adverse consequences for some or all Victorians → large-scale economic consequences to Victoria.	Department or government agency's internal cyber security incident response plan, enacted internally	State Emergency Management Plan Cyber Security Sub-Plan (the Sub-Plan), enacted by the Control Agency Officer in Charge (Secretary, DGS)	Notification is required to: → CIRS via the Whole of Victorian Government Cyber Security Portal or 1300 278 842 (if outside of business hours) → other stakeholders, as per the Sub-Plan

3 Introduction to arrangements

3.1 Our collective cyber security vision

Cyber security incidents threaten Australia's national security. Incidents can impact the economy, the environment and community safety.

The Commonwealth Government's 2023–2030 Australian Cyber Security Strategy promotes national cyber-resilience. It aims to make Australia a world leader by 2030.

At a state level, the vision of Victoria's Cyber Strategy 2021 is to create a cyber safe Victoria. The vision is achieved through 3 core missions:

1. the safe and reliable delivery of government services
2. a cyber safe place to work, live and learn
3. a vibrant cyber economy

3.2 Shared responsibility

Building resilient, cyber safe communities is a shared responsibility.

- The Department of Government Services (DGS) leads the state's cyber security arrangements.
- Partnerships (between government, industry, community and academia) are key to protecting Victorians online.
- Individuals are encouraged to learn about and reduce their own cyber security risk.

3.2.1 Department of Government Services and Cyber Incident Response Service

- This plan outlines responsibilities for the department, including the Victorian Government Cyber Incident Response Service (CIRS) and the Victorian Government Chief Information Security Officer (CISO).

3.2.1.1 Introducing the Victorian Government Cyber Incident Response Service

DGS leads the state's response to cyber security incidents through the CIRS. CIRS operates a cyber security incident and threat intelligence response service. CIRS prioritises its response in line with the State Emergency Management Priorities (see **Appendix D**). The service exists to help departments and government agencies to limit the effects of cyber security incidents and cyber threats. CIRS provides departments and government agencies with advice and supplementary support that aligns with the contents of this plan.

3.2.1.2 Cyber Incident Response Service's scaled response model

CIRS can provide supplementary support to a department or government agency for any of its identified responsibilities in this plan, subject to CIRS' capacity and capability. In all instances, CIRS will use a scaled response model to prioritise Victorian Government resources. The first priority is emergencies, then critical cyber security incidents, followed by major incidents, then limited incidents.

To ensure as much consistency as possible in WoVG cyber security arrangements, CIRS adopts the State Emergency Management Priorities at both incident and emergency level. CIRS prioritises its response in line with the State Emergency Management Priorities (see **Appendix D**).

Departments and government agencies are also encouraged to consider additional avenues for support, where appropriate and as required.

3.3 About this plan

Responding to cyber security compromises across the 6 levels of severity requires different plans (see **Table 2**). Each department and government agency should print a physical copy of each plan so they can still access this information even if internal systems are compromised.

All plans work together. Each plan focuses on a different audience (either a specific department or government agency, or WoVG), and covers the different severities of cyber security compromise. All plans are required to outline relevant activities for before, during and after a cyber security compromise (see Figure 1).

FIGURE 1: Phases across time

TIMELINE

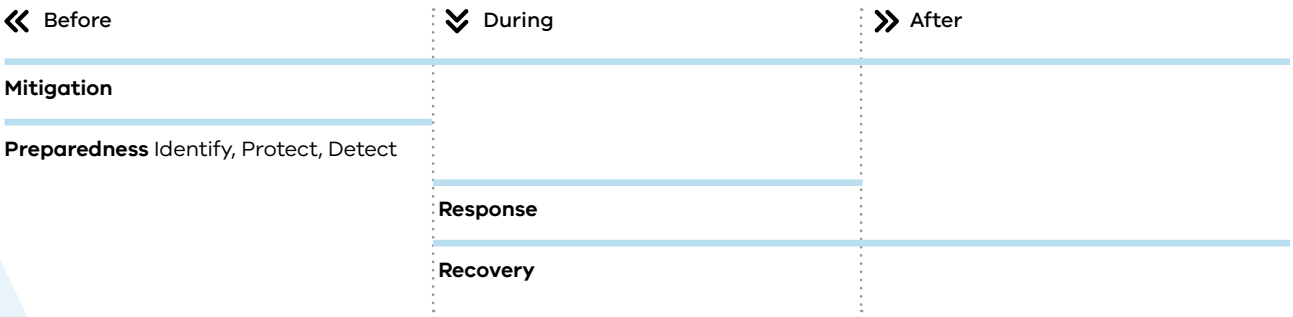


TABLE 2: Overview of internal and WoVG cyber security plans

Severity (low to high)	WoVG category	Relevant internal plan	Relevant WoVG plan	Arrangements	Plan preparer	Overview of the plan
1	Event	Cyber security incident response plan	This severity level does not require a WoVG approach. Each department and government agency must arrange its own approach.	Internal incident response plans should cover all severities of impact, ranging from a cyber security event (severity level 1) to cyber security emergency (severity level 6).	The relevant department or government agency.	An individualised plan allows the entity to respond to cyber security events, incidents and emergencies as they chose. It should reflect similar structure and core content as both WoVG plans for consistency. DGS provides an optional template to support this.
2	Minor					
3	**Limited**	Cyber security incident response plan	**This Plan**	This plan supports WoVG arrangements for, including DGS' leadership of, limited, major or critical non-emergency cyber security incidents. It is enacted alongside the department or government agency's internal plan. Where there is the threat of an incident of this severity that does not eventuate, it is the responsibility of each department and government agency to determine which of this plan's activities are relevant.	The Victorian Government CISO, DGS as lead for the Victorian Government's cyber security arrangements.	It is based on the structure and content of the Sub-Plan. This creates consistency in the WoVG management of cyber security incidents and emergencies.
4	**Major**					
5	**Critical**					
6	Emergency	Cyber security incident response plan	The Sub-Plan	If a cyber security emergency is declared, the Sub-Plan takes precedence over the arrangements outlined in this plan. The Sub-Plan supports DGS and the Emergency Management Commissioner to provide leadership in cyber security emergencies. The mitigation and preparedness sections in the Sub-Plan are similar across that and this plan. It is enacted alongside the department or government agency's internal plan.	DGS, as the Control Agency for cyber security emergencies, on behalf of the Emergency Management Commissioner. It is one of the State Emergency Management Plan sub-plans under Victoria's emergency management planning framework (*Emergency Management Act 2013* (Vic)).	The Minister for Emergency Services' *Guidelines for Preparing State, Regional and Municipal Emergency Management Plans* requires the Sub-Plan to outline mitigation, response and recovery, as well as roles and responsibilities.

3.4 Wider state and federal government arrangements

This plan aligns with cyber security and emergency risk management arrangements at the state and federal level.

TABLE 3: Victoria's cyber security management framework.

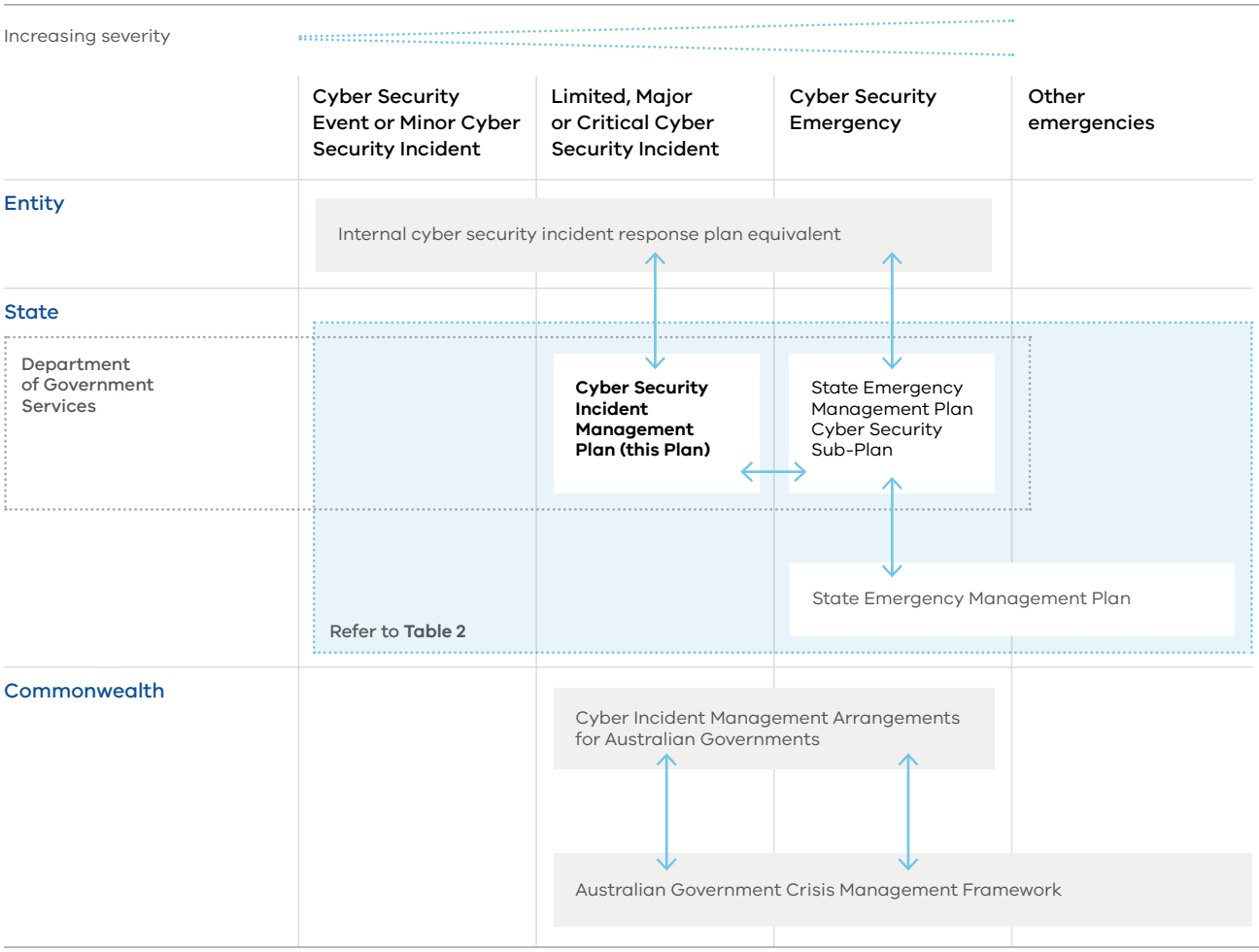


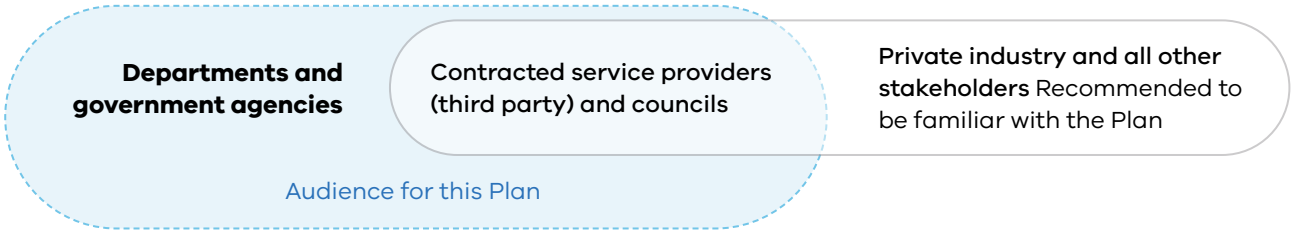
Table continues next page.

Table starts on previous page.

Level	Arrangement	Issued by	Summary
Department or government agency	Internal cyber security incident response plan equivalent	Department or government agency	Refer to **Table 2**
State	**This Plan**	DGS	Refer to **Table 2**
	The Sub-Plan	DGS on behalf of the Emergency Management Commissioner	Refer to **Table 2**
	Victoria State Emergency Management Plan	Emergency Management Commissioner	This outlines Victoria's arrangements for the mitigation of, preparedness for, response to and recovery from all major emergencies as well as agency roles and responsibilities.
Commonwealth	Cyber Incident Management Arrangements for Australian Governments	National Cyber Security Committee (NCSC)	These arrangements aim to bring different levels of government together to reduce the scope, impact and severity of national cyber security incidents.
	Australian Government Crisis Management Framework	Department of Prime Minister and Cabinet	This outlines how the Australian Government manages crises. This involves an 'all-hazards' approach from prevention to recovery that includes assisting states and territories. It outlines roles and responsibilities for ministers and senior officials.

3.5 Audience

FIGURE 2: Overview of the audience for this plan



This plan is primarily written for Victorian departments and government agencies to use. All other users of this plan should assume the responsibilities for 'departments and government agencies' apply to them, unless there is clear justification to proceed otherwise.

3.5.1 Departments and government agencies

In this plan, the term 'departments and government agencies' covers:

- public service bodies, including all Victorian Government departments
- government agencies
- public entities[1]
- special and exempt bodies, except for councils[2]
- public sector infrastructure owners and operators.[3]

3.5.2 Contracted service providers ('third parties')

Departments and government agencies must ensure that a contracted service provider does not contravene a protective data security standard in respect of public sector data collected, held, used, managed, disclosed or transferred by the contracted service provider.[4]

Departments and government agencies are responsible for ensuring that contracts with contracted service providers ensure that cyber security risk is managed in line with the risk and the value of the information or service. This includes but is not limited to ensuring that the relevant aspects of this plan are adhered to by the contracted service provider, such as implementation of the appropriate maturity models and frameworks outlined in this plan.

1 As defined in section 5 of the *Public Administration Act 2004* (Vic).
2 As defined in section 4 of the *Public Administration Act 2004* (Vic).
3 Critical infrastructure sectors are identified by the Victorian Critical Infrastructure Strategy. Note that references to the *Security of Critical Infrastructure Act 2018* (Cth) in this plan are applicable to a similar but different list of critical infrastructure responsible entities, as defined under that legislation.
4 Section 88 of the *Privacy and Data Protection Act 2014* (Vic).

Contracted service providers must adhere to the clause agreements set out in their contracts. Contracts should require cooperation with this plan, especially for providers that work with systems, services or information on the state's behalf.

Departments and government agencies who engage a managed or contracted service provider may outsource the delivery of responsibilities under this plan. However, the department or government agency remain accountable for the responsibility.

Contracted service providers include those that are also Victorian public service bodies (for example, Cenitex).

3.5.3 Councils

Victoria's councils are encouraged to adopt this plan. Councils may manage cyber security incidents using strategies outlined in sections labelled 'departments and government agencies'. Councils may also seek support from DGS. Each council should consider this plan in its own internal cyber security planning.

3.5.4 Private industry entities

Private industry entities include:

- private critical infrastructure owners and operators
- businesses
- non-government community service organisations or providers
- not-for-profit organisations.

This plan acknowledges Commonwealth laws and regulations relating to private industry, including those contained in the *Privacy Act 1998* (Cth) and the *Security of Critical Infrastructure Act 2018* (Cth).

Private industry entities should follow this plan when a cyber security incident may directly or indirectly impact departments and government agencies.

Private industry entities must follow this plan where it relates to Commonwealth or Victorian laws or responsibilities, or there are contractual responsibilities as a contracted service provider.

3.5.5 Other stakeholders

All other stakeholders can consider this plan to see how it might be useful in setting out internal roles and responsibilities. Other stakeholders may include:

- interested Victorian community members
- governments of other states and territories
- the Commonwealth Government, including:
  - Australian Cyber Security Centre (ACSC)
  - National Office of Cyber Security (NOCS)
  - National Cyber Security Coordinator

- National Emergency Management Agency (NEMA)
- Department of Home Affairs
- National Cyber Security Committee (NCSC).

Although there may be members of the Victorian community who are interested in this plan and its application, the plan does not identify individual roles or responsibilities.

3.6 State significant risk

Cyber security incidents can pose a significant risk to the state. The Victorian Government's State Significant Risk Interdepartmental Committee recognises cyber incidents as a state significant risk.[5] This means there are potential statewide consequences or impacts for community, government and private industry.

Additionally:

- Emergency Management Victoria's Emergency Risks in Victoria assessment includes cyber security as an emergency risk.
- Victoria has 8 critical infrastructure Sector Resilience Networks (SRNs) (see **Appendix E**). Each is led by a government department which prepares a plan once a year. At the time of this plan's publication, all Sector Resilience Plans identify cyber security incidents as a risk.

3.7 Core expectations

All departments and government agencies are expected to manage cyber security incidents by:

- following Victorian and Commonwealth cyber security legislation or guidelines
- implementing an industry recognised best practice approach to cyber security
- maintaining and exercising internal incident arrangements
- protecting cyber security environments against threats and applying relevant regulatory controls
- ensuring internal capability and capacity to respond to a cyber security incident or threat
- responding quickly to changes in threat, incidents and consequences
- working with CIRS before, during and after cyber incidents, where relevant
- using the State Emergency Management Priorities (see **Appendix D**) to guide decisions during response.[6]

5 The term 'cyber incidents' used in the state-level emergency risk assessment is considered interchangeable with the term 'cyber security incidents' used in this plan.

6 To ensure as much consistency as possible in WoVG cyber security arrangements, the Victorian Government adopts the State Emergency Management Priorities at both incident and emergency level.

4 Cyber security incident mitigation

Mitigation is the elimination or reduction of the incidence or severity of a cyber security compromise, and the minimisation of its effects.[7]

4.1 Improving cyber security maturity

4.1.1 Summary

Many cyber security incidents are traced back to a low level of cyber security maturity in one or more areas. This makes it easier to be exploited by a threat actor. A threat actor may be external to the department or government agency, or internal.

It is important to manage risks to the confidentiality, integrity and availability of digital systems, services and information.

Activities to improve maturity should reflect the level of risk the department or government agency holds.

See **Appendix F** for a list of frameworks referenced in this sub-section.

4.1.2 Roles and responsibilities

4.1.2.1 Departments and government agencies

- Adopt one (or some elements of both) of these maturity models/frameworks:
  - ACSC's Essential Eight Maturity Model (E8)[8]
  - National Institute of Standards and Technology (USA) Cyber Security Framework (NIST).

7 Adapted from the Victorian SEMP.

8 In line with ACSC's guidance regarding the Essential 8, departments and government agencies may consider additional mitigation strategies and controls can be considered, including those from the *Strategies to Mitigate Cyber Security Incidents* and the *Information Security Manual*.

- Consider their risk profile or an agreed industry standard when determining the right level of maturity to apply.
- Apply, as required:
  - the Victorian Protective Data Security Framework and Standards as per the *Privacy and Data Protection Act 2014* (Vic) or other relevant standards if necessary
  - the Information Security Manual when holding and accessing Commonwealth Government sensitive and security classified information
  - requirements under the *Security of Critical Infrastructure Act 2018* (Cth)
  - the Victorian Government Risk Management Framework (VGRMF)
  - the Australian Energy Sector Cyber Security Framework (for the energy sector)
  - the *Health Records Act 2001* (Vic) if necessary to protect the privacy of individuals' health information (for the health sector).

4.1.2.2 Department of Government Services

- Promote a culture of cyber-resilience through the creation and implementation of Victoria's Cyber Strategy.
- Engage departments and government agencies on opportunities to implement Victoria's Cyber Strategy through their portfolios.
- Support departments or government agencies to assess the level of cyber security maturity they need.

4.1.2.3 Department of Home Affairs (Commonwealth)

- Deliver the 2023–2030 Australian Cyber Security Strategy.
- Regulate cyber and critical infrastructure security, through the Cyber and Infrastructure Security Centre (CISC).

4.2 Threat intelligence

4.2.1 Summary

Threat intelligence is the collection, analysis and reporting of an adversary's motive, intent and capabilities. It is also used to assess the potential threat posed by the exploitation of vulnerabilities or a threat actor's tactics, techniques and procedures. Threat intelligence allows departments and government agencies to make timely and informed cyber security decisions to prevent an attack in progress, or mitigate against future attacks. It provides an early warning of emerging or existing threats or hazards in the cyber environment.

Appropriate classification and caveats need to be used to ensure intelligence is shared within a secure information security governance framework. To ensure information is shared with the appropriate audience, DGS uses the ACSC's Traffic Light Protocol (TLP). However, this protocol does not replace protective markings or information management markers. TLPs must be adhered maintain the integrity of information sharing arrangements across the cyber security community.

TABLE 4: Disclosing threat intelligence with the TLP

Traffic light protocol	Meaning
Red	Not for disclosure, restricted to recipients only
Amber + Strict	For limited disclosure, restricted to recipient's entity only
Amber	For limited disclosure, restricted to recipients' entity and its clients or contractors
Green	Can be disseminated to recipients' stakeholders as deemed necessary
Clear	Disclosure is not limited

A summary of intelligence products and reports appears at **Appendix G**.

4.2.2 Roles and responsibilities

4.2.2.1 Departments and government agencies

- Review threat intelligence issued by CIRS to assess and detect potential exposure and implement mitigations as required.
- Share information and intelligence with CIRS to support CIRS to manage the flow of threat intelligence across departments and government agencies.
- Share threat intelligence with relevant SRN chair/s as well as contracted service providers and managed service providers (MSPs), if suitable under the given TLP.
- Report confirmed detections to CIRS. Once validated, CIRS may share threat intelligence with other Victorian Government stakeholders, Victoria Police, state and territory jurisdictions and the ASD's ACSC, to minimise the harm to Australian cyber infrastructure and the community.

4.2.2.2 Department of Government Services

- Coordinate and share threat intelligence from Commonwealth Government, interstate jurisdictions and Victoria with Victorian departments and government agencies.
- Share risk mitigation guidance with departments and government agencies via alerts and advisories (See **Appendix H**).
- Develop a WoVG threat picture to inform stakeholders.
- Collect and share technical information about incidents to inform WoVG response efforts, including liaison with ASD's ACSC, Victoria Police and state and territory jurisdictions.
- Collect, analyse and report tactical, technical, operational and strategic intelligence to support incident response activities.
- Identify emerging threats and trends to inform strategic planning and decision-making when assessing the cyber security risk posed to departments and government agencies.
- Share Victorian threat intelligence with Australian governments central cyber divisions.
- Participate as a member of the NCSC National Operations Sub-Committee (NOSC).[9]

9 NOSC comprises central government and state and territory representatives, ASD's ACSC, the National Office of Cyber Security and the Australian Federal Police. It shares cyber incident and threat intelligence. This cohort also participates in national technical and consequence management forums for national cyber incidents.

4.2.2.3 Sector Resilience Network chairs

→ Provide threat intelligence to its SRN membership[10] and key stakeholder groups as per the TLP.

4.2.2.4 Australian Cyber Security Centre[11]

→ Share threat intelligence with CIRS to ensure appropriate mitigation activities can be implemented to prevent the realisation of an impact to Victorian Government infrastructure, the delivery of Victorian Government services and the Victorian community.

4.3 Community and industry awareness and engagement

4.3.1 Summary

For community and industry[12] to improve their cyber security, they must receive timely, relevant and tailored advice and support to assist decision-making and minimise related harms.

4.3.2 Roles and responsibilities

4.3.2.1 Department and government agencies

→ For incident-specific communications, refer to the media and public communications section.

4.3.2.2 Department of Government Services

→ In partnership with key departments and government agencies, including Victoria Police, lead initiatives which foster a cyber resilient Victorian community, aligned to the vision and objectives of Victoria's Cyber Strategy 2021 or equivalent.

4.3.2.3 Department of Jobs, Skills, Industry and Regions

→ In partnership with key departments and government agencies, including DGS, lead initiatives which foster cyber resilient Victorian businesses, aligned to the vision and objectives of Victoria's Cyber Strategy 2021 or equivalent.

10 This includes private industry and public sector critical infrastructure owners and operators. See **Appendix E** for more information on SRNs.
11 The Commonwealth Government receives highly classified information from intelligence agencies and international partners to assist Australia's detection and response to cyber security threats. This intelligence is shared, on a need-to-know basis with State and Territory governments.
12 Industry' in this section means industry more generally. It is not a specific reference to critical infrastructure owners and operators.

5 Cyber security incident preparedness (identify, protect and detect)

Preparedness includes the activities to prepare for and reduce the effects of a cyber security compromise by having plans, capability and capacity for response and recovery.[13]

5.1 Identify and protect from cyber security risk

5.1.1 Summary

In preparedness for a cyber security incident, departments and government agencies must develop maturity to manage cyber security risks to, and perform actions to ensure, the confidentiality, integrity or availability of information, systems or services.[14]

5.1.2 Roles and responsibilities

5.1.2.1 Departments and government agencies

- Identify threats, vulnerabilities and risks to the confidentiality, integrity or availability of information, systems or services.
- Follow the 5 steps in OVIC's action plan to:

1. identify information assets
2. determine the 'value' of this information
2. identify any risks to this information
4. apply security measures to protect the information
5. manage risks across the information lifecycle.

13 Adapted from the SEMP.
14 Modified from the NIST Framework.

- Establish cyber security policies with clear roles and responsibilities.
- Document critical processes, asset details, network topographies and key contacts.
- Maintain an up-to-date list of hardware and software, including cloud-based applications and virtual infrastructure.
- Develop playbooks and business continuity plans in case critical assets need to be taken offline, with consideration to disaster recovery and initial actions required (e.g. first 72 hours).
- Regularly train and retrain users of specific cyber security policies and procedures, especially those with roles and responsibilities identified in those procedures.
- Review cyber insurance arrangements at least annually.

5.1.2.2 Department of Government Services

- Provide advice, guidance and centralised cyber security services to departments and government agencies.

5.2 Maintain and exercise plans and arrangements

5.2.1 Summary

As part of their preparedness, departments and government agencies are responsible for preparing, reviewing, exercising and updating their own internal cyber security incident response plan and arrangements.

5.2.2 Roles and responsibilities

5.2.2.1 Departments and government agencies

- Create a cyber security incident response plan that aligns with this plan, the Sub-Plan, the Victorian Protective Data Security Framework/Standards,[15] any sector specific frameworks and best practice.[16] The plan is to outline roles and responsibilities and arrangements to mitigate, prepare, respond and recover from a cyber security compromise.
- Conduct an annual exercise of the plan.[17] An exercise may be as simple as an internal discussion, or as a detailed multi-agency deployment-style exercise. Exercises may include cyber and emergency management personnel, multi-agency stakeholders (such as critical infrastructure) or relevant community members and groups. Any areas for improvement identified in exercises must be considered at the point that the cyber security incident response plan is next updated.

15 This relates specifically to VPDSF/S Standard 6, to 'establish, implement and maintain an information security incident management process relevant to size, resources and risk posture.'
16 Optional template available at Cyber Incident Response Plan template.
17 The ACSC has prepared 'Exercise in a Box' scenario resources to help entities run exercises for this reason.

- Create and regularly review supporting incident response processes and procedures.
- Educate management about the roles of executive and senior management in the plan.
- Assess internal capability and capacity for the identified roles and responsibilities in the plan, processes and procedures and address identified gaps. For example, maintaining sustainable staffing of an incident response may require:
  - engaging a contracted service provider to supplement internal capability and capacity
  - engaging an insurance provider to see what additional resources are available.

5.2.2.2 Department of Government Services

- Maintain the WoVG cyber security incident management arrangements and capability (outlined in this plan and the Sub-Plan).
- Educate stakeholders on the WoVG cyber security arrangements.
- Conduct at least one exercise of this plan annually.
- Review and update this plan at least every 3 years, using the outcomes of annual exercises to improve the plan.
- Publish a cyber security incident response plan template for the optional use of departments and government agencies. Use of the template will support alignment with the arrangements set out in this plan.
- Provide support for department and government agencies' cyber security exercises where resourcing allows.

5.3 Detection

5.3.1 Summary

To protect systems and data from cyber security threats, real-time monitoring to detect threats, security risks and controls associated with systems and the operating environment is essential to maintaining a department or government agency's security posture.

One of the core elements of detecting and investigating cyber security incidents is the availability of appropriate data sources, such as event logs. Event logs can be used by a department or government agency to assist with detecting and investigating cyber security incidents. Event logs include cross domain solutions, databases, domain name system services, email servers, gateways and multifunction devices. Further recommendations can be found in the Information Security Manual.

5.3.2 Roles and responsibilities

5.3.2.1 Departments and government agencies

- Continuously monitor assets to find anomalies, indicators of compromise and other potentially adverse events.
- Ensure appropriate logging and monitoring capability is in place to detect, understand and analyse event logs and identify cyber security incidents.
- Liaise with the respective MSPs to ensure threats are detected, analysed, communicated and managed consistent with the intent of this plan, where MSPs are used to provide threat detection and analysis services.
- Update resources to ensure access to the latest:
  - network diagrams
  - IP addressing schemas
  - port lists
  - system logs
  - documentation that may include system designs/architecture, security plans and GPO configuration.
- Review log entries and security alerts to determine if there are any unusual entries or signs of suspicious behaviour on the network or applications.
- Develop standard operating procedures for different operating systems on what to look for or review (such as, specific event log sources, the types of events to search for).
- Consult with network and application experts to determine if there is a legitimate explanation for unusual or suspicious activity.
- Research and review any open-source materials (including via internet search engines) relating to unusual or suspicious activity. For example, perform a search on any unusual filenames on the network.
- Develop a watch list/monitor list of suspected accounts or IPs to monitor their ongoing activity.
- Conduct investigations securely through a contracted service provider.

- **IMPORTANT: Do not 'ping' or try to communicate with a suspected IP address or URL from your own network. This may tip off the attacker that you have detected their activity. A contracted service provider can conduct this activity securely and anonymously.**

5.3.2.2 Department of Government Services

- Monitor cyber security threats that may impact Victoria's assets.
- Share timely information and intelligence with departments and government agencies as they are affected by incidents or threats.
- Liaise with the ACSC and other state and territory jurisdictions.

6 Cyber security incident response

Response is the action taken immediately before, during and in the first period after a cyber security compromise to reduce the effects and consequences of the incident.[18]

6.1 Analysis

6.1.1 Summary

Departments and government agencies will consider all indicators of a cyber security compromise and potential threats to confirm, as quickly as possible, whether a compromise has occurred or is occurring.

6.1.2 Roles and responsibilities

6.1.2.1 Department or government agency

- Undertake initial analysis to:
  - determine scope, impact and severity of a cyber security compromise (in line with **Table 1**)
  - commence incident notifications (See 'Notification and classification' section).
- Undertake further analysis. While incident notifications and other response activities are being completed, a more detailed analysis can continue to:
  - assess the BIL (see **Appendix C**)
  - collect and record evidence to support forensic investigations. Such evidence may include:
    - hard drive images, raw images and RAM images
    - IP addresses
    - network packet captures and flows
    - network diagrams

18 Adapted from the SEMP.

- log and configuration files[19]
- databases
- incident response and investigation notes
- screenshots
- social media posts
- CCTV, video and audio recordings
- documents detailing the monetary cost of remediation or loss of business activity
- collate and securely store all collected evidence
- create and maintain a log of all evidence collected. This log should include:
  - date and time collected
  - name of person who collected it
  - details of each item
- ensure all access to evidence is recorded, including the reason for access. This is important in maintaining the 'chain of custody' for collected evidence
- record details of transfers. Limit the evidence transferred between staff.

6.1.2.2 Department of Government Services

- Support departments and government agencies with their incident response, forensic analysis and threat intelligence, where it is beyond the capacity or capability of the impacted department or government agency.

6.2 Notification and classification

6.2.1 Summary

Departments and government agencies have specific responsibilities to notify their key stakeholders about events, incidents and emergencies. Notification to CIRS should commence as soon as the compromise has been confirmed.

Cyber security incidents are categorised based on potential or actual impacts. CIRS uses a 6-tier model to categorise the severity level of WoVG cyber security threats and incidents. The 6-tier model is provided in detail in **Table 1** and summarised in **Table 5** below. **Appendix C** shows how the categories can be seen as a state-level equivalent to the OVIC entity-level Business Impact Levels (BILs).

The more severe the category, the more formally and extensively all actions in the response phase of this plan should be completed.

Once classified, notifications should be handled according to the categorisation of the incident. Sensitivity and confidentiality should align with the TLP assigned to the incident.

See **Figure 3** for notification responsibilities and **Appendix H** for contact details of common stakeholders to notify.

19 Refer to the Victorian Government Log Collection and Retention Guidelines, available from DGS.

Classified incident notifications must be strictly managed in accordance with information security policies. Access to briefings and materials containing classified material must only be shared with persons holding an appropriate clearance and with an official need to access the information.

Notification to affected individuals is covered under the 'media and public communication' section.

6.2.2 Roles and responsibilities

6.2.2.1 The detecting department or government agency

- Inform the impacted department or government agency as soon as possible. This responsibility applies to any department or government agency (including DGS) that detects the compromise first.

6.2.2.2 Impacted department or government agency

- Notify CIRS. The primary method of notifying CIRS is via the Whole of Victorian Government Cyber Security Portal, or phone (1300 278 842) if outside of business hours. If notification is given via the phone, a written notification via the Portal must be made within 72 hours, or 12 hours if it is classified as a major or critical incident.
- Make the notifications outlined in Figure 3 and its explanatory notes, in line with the given classification after CIRS has confirmed the WoVG classification. The impacted department or government agency **should not** notify any additional stakeholders.

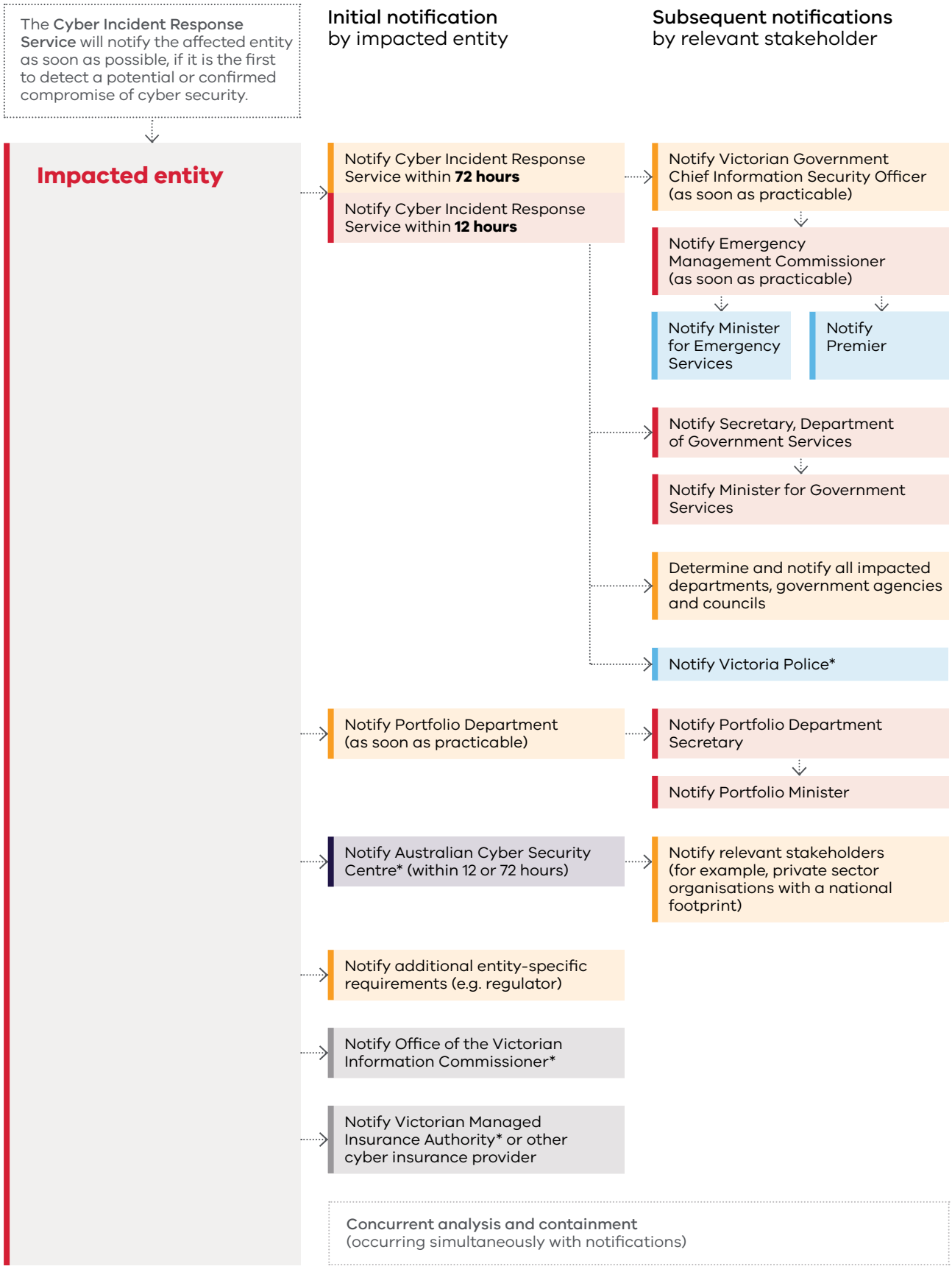
6.2.2.3 Department of Government Services

- Confirm the WoVG categorisation of any limited, major or critical cyber security threat or incident, in alignment with **Table 5**. Consider any advice from the:
  - impacted department or government agency
  - relevant portfolio government department
  - National Cyber Security Committee (NCSC).

TABLE 5: Categorisation for WoVG

Severity level	WoVG category	Authority to categorise this severity level
1	Event	Within the impacted department or government agency
2	Minor	
3	**Limited**	DGS
4	**Major**	
5	**Critical**	
6	Emergency	Control Agency Officer in Charge (Secretary, DGS)

FIGURE 3: Notification responsibilities for limited, major, and critical cyber security incidents



- Required notification for all incidents
- Required notification for major and critical incidents only
- Where required by *Security of Critical Infrastructure Act 2018* (Cth)
- At the discretion of the preceding stakeholder
- Required where relevant to the stakeholder

*Additional comments on page 27

Table of contents

6.2.3 Explanatory notes for Figure 3

6.2.3.1 Notification to Cyber Incident Response Service

Early notification to CIRS is required to ensure the incident is classified in accordance with this plan. The classification will determine stakeholder notifications and resourcing.

While CIRS assistance may not be required, notifications enable CIRS to maintain situational awareness and a WoVG visibility of the cyber security threat and incident landscape. Additionally, notifications assist CIRS to identify multi-organisation cyber security incidents and enacts its coordination responsibility.

In addition to regulatory reporting obligations, private industry critical infrastructure owners and operators should notify CIRS and operational stakeholders of the relevant portfolio department of any about any supply or service delivery disruptions arising from a cyber security incident that are likely to impact Victorians.

6.2.3.2 Notification to portfolio department

Victorian Government administrative offices, special bodies and public entities are to notify their relevant portfolio department of cyber security incidents in a timely manner. Portfolio departments will provide guidance on notification arrangements.

A list of public sector portfolio departments is available on the Victorian Public Sector Commission website.

6.2.3.3 Notification to Australian Cyber Security Centre

As per the *Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act), critical infrastructure owners and operators (as determined under SOCI Act) must notify ACSC within:

- 12 hours if the incident has had or is having a 'significant impact' on the availability of an asset[20]
- 72 hours if the incident has had, is having or is likely to have, a 'relevant impact' on an asset[21].

Notifications that the impacted department or government agency provide to the ACSC are not forwarded to Victorian Government.

6.2.3.4 Notifications to regulators

The impacted department or government agency is responsible for acquitting notifications in line with its regulatory obligations.

20 As defined in section 30BEA of the SOCI Act, a 'significant impact' is one where both the critical infrastructure asset is used in connection with the provision of essential goods and services; and the incident has materially disrupted the availability of the essential goods or services delivered by a critical infrastructure asset or any of the circumstances specified in the rules exist in relation to the incident.

21 As defined in section 8G of the SOCI Act, a 'relevant impact' is an impact of the hazard on the availability, integrity, reliability or confidentiality of your asset.

6.2.3.5 Notifications to the OVIC

Departments and government agencies subject to the VPDSF/S must notify the OVIC within 30 days if the incident compromises the confidentiality, integrity or availability of public sector information. This is a requirement at BIL 2 (**Appendix C**), as per the Victorian Protective Data Security Framework/Standards.

DGS' Memorandum of Understanding with the OVIC allows CIRS to notify the regulator on behalf of departments and government agencies subject to the *Privacy and Data Protection Act 2014* (Vic). This provides early advice of data breaches to the OVIC.

6.2.3.6 Notifications to the Victorian Managed Insurance Authority or other cyber insurance provider

The Victorian Managed Insurance Authority (VMIA) or other cyber insurance provider should be notified as soon as possible to assist the impacted department or government agency response and recovery efforts. The department or government agency should contact their insurer before incurring significant costs for response and/or notification.

6.2.3.7 Victoria Police

DGS works closely with Victoria Police to share information and intelligence about cyber security incidents affecting the Victorian Government. DGS will refer to Victoria Police all incidents that are suspected criminal offences. Departments and government agencies may also refer incidents to Victoria Police via Report Cyber.

6.2.3.8 Emergency Management Commissioner

The Emergency Management Commissioner must be notified if a cyber security incident has the potential to become a cyber security emergency.

6.3 Technical response, including containment and eradication

6.3.1 Summary

During a cyber security incident, the technical response addresses the root cause of the cyber security compromise.

Appendix B provides a list of common cyber security incident types and impacts, along with typical response activities to minimise potential harm specific to that type or impact.

6.3.2 Roles and responsibilities

6.3.2.1 Impacted department or government agency

- Lead its own technical response.
- Complete analysis (See the **Analysis** section).
- Develop and implement an internal incident response plan which details containment, eradication and recovery activities.
- Seek assistance from CIRS if more resources are needed.

6.3.2.2 Department of Government Services

- Manage the CIRS response.
- Support the impacted department or government agency to create and oversee the implementation of its internal incident response plan.
- Connect the impacted department or government agency with expert people, tools, services and knowledge to assist. This may require requesting support from the following support agencies:
  - relevant Victorian departments, government agencies[22]
  - Commonwealth-level departments or agencies, including ACSC
  - private industry cyber security providers, for expert technical advice or forensic services.

6.4 Control and coordination

6.4.1 Summary

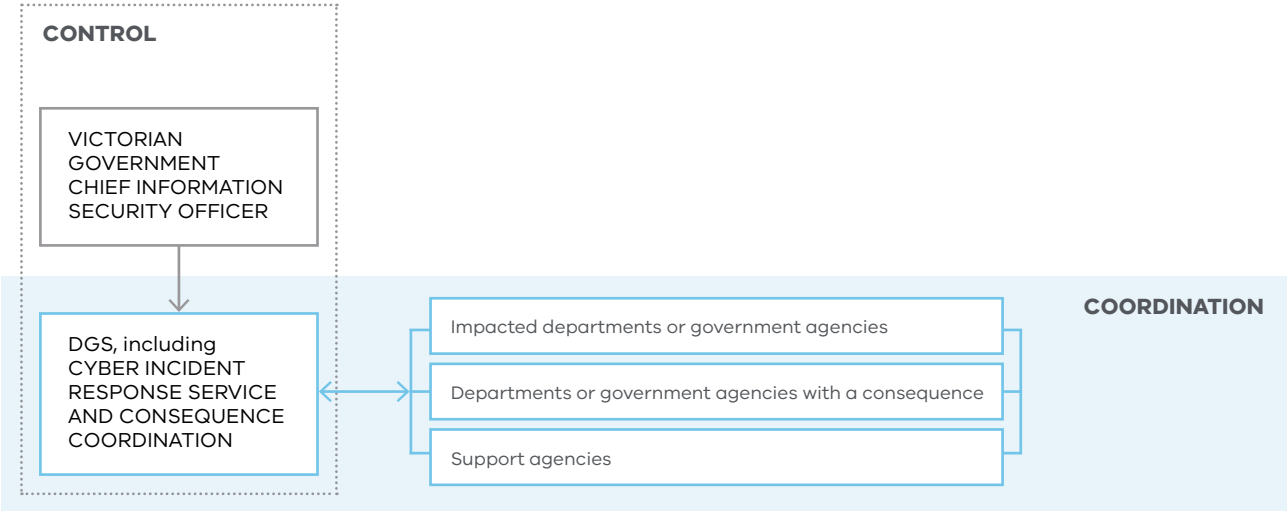
Control refers to the directing of response activities across departments and government agencies. This includes the coordination and tasking of other agencies.

Coordination is the bringing together of people, resources, governance, systems and processes to ensure effective response and recovery. A well-coordinated response needs two-way communication between all affected stakeholders.

Stakeholders should communicate in such a way that helps other stakeholders to meet their own areas of responsibility.

22 As per the SEMP's Table 10.

FIGURE 4: Control and coordination



6.4.2 Roles and responsibilities

6.4.2.1 Impacted department or government agency

- Lead its own response to resolve the incident using internal resources. Seek assistance from CIRS if more resources are needed.
- Appoint an incident manager and advise CIRS.
- Maintain a written record of decisions made throughout the duration of the incident.
- Follow, where useful, the incident management guidelines set out in the Australasian Inter-Service Incident Management System (AIIMS) (See **Appendix I**). This may include creating an internal incident management team to delegate roles to.

6.4.2.2 Department or government agency

- Assist as a support agency in line with portfolio responsibilities. This may include ensuring the continuation of normal services or a specific response or relief activity.

6.4.2.3 Department of Government Services

- Develop a WoVG view of the incident.
- Manage and monitor the WoVG response to any:
  - multi-department or government agency cyber security incident
  - incident that affects MSPs or contracted/shared service providers used by multiple departments or government agencies.
- Develop a WoVG incident action plan if needed, including consequence management.
- Establish, where useful, management arrangements to make an integrated response possible.

- Collaborate with all relevant departments and government agencies to provide effective leadership and coordination of response activities.
- Coordinate activities of departments or government agencies with roles or responsibilities in relation to incident response.
- Prepare and circulate communications (including threat intelligence and SITREPs) to support any briefings required:
  - within DGS, including for the Victorian Government CISO and DGS Secretary
  - for the Minister for Government Services
  - for CISOs and incident managers of the:
    - impacted department/s and government agency/ies
    - all other relevant departments and government agencies
  - for affected private industry
  - for the Emergency Management Commissioner (only for major and critical cyber security incidents).
- As needed, engage with:
  - ACSC
  - critical infrastructure SRNs, via the Critical Infrastructure Resilience Sectors Forum
  - law enforcement agencies (e.g. Victoria Police)
  - National Cyber Security Committee (NCSC)
  - OVIC.

6.5 Consequence management

6.5.1 Summary

Consequence management relates to the follow-on impacts of cyber security incidents. Victoria categorises incidents based on the consequences they have for Victorians (see **Table 1**).

Consequence management requires a response to include both:

- a department or government agency with compromised cyber security
- secondary and subsequent impacted departments or government agencies. These are any additional departments or government agencies impacted by the compromise (e.g. interdependencies or non-technical impacts on the community).

6.5.2 Roles and responsibilities

6.5.2.1 Department or government agency with a consequence

- Manage its own response to any consequence.
- Liaise with relevant stakeholders.
- Create and enact an action plan to address the consequences for areas of portfolio responsibility.
- Activate business continuity plans as needed.
- Contact insurance provider for guidance (e.g. on evidence collection, relief activities and level of support required).
- Support the coordination and management of impacts and consequences through provision of appropriate functional advice, leadership and information to DGS convened coordination forums, such as the Consequence Coordination Team (CCT). The advice should:
  - identify impacts
  - identify actual, emergent and related consequences and related actions
  - form the basis of intelligence used to brief other WoVG stakeholders
  - be available to other departments and government agencies who can use this information to brief Ministers and senior staff
  - provide advice on public and industry messaging.
- Ensure adequate internal arrangements are established to enable timely and accurate reporting of consequences.
- Log any unresolved risks in an internal risk register. Manage in accordance with the internal risk management framework.
- Lead engagement, as required, with relevant external stakeholders (including private industry) to support WoVG incident response and consequence management messaging.

FIGURE 5: How a cyber security incident can have consequences for other entities

6.5.2.2 Department of Government Services

- Lead the coordination of consequences where the incident affects multiple departments and government agencies or when there are significant impacts to the Victorian community.
- Consider consequences and how they are being managed in decision-making.
- Engage early with departments and government agencies to identify potential consequences. Where appropriate, this may include leading a Consequence Coordination Team (CCT) meeting to:
  - identify the potential consequences at state level
  - develop a state strategic plan with high-level mitigation and response actions for departments and government agencies to manage consequences and reduce impacts on Victorians, if required.
- Seek information from SRNs. Requests for information should be detailed in context, specific as to what the request is, and include what audience the information will be provided to.
- Request assistance from support agencies:
  - relevant Victorian departments and government agencies
  - Commonwealth-level departments or agencies, including the ACSC.

6.5.2.3 Sector Resilience Networks

- Provide information to and from industry network members to inform DGS' decision-making.
- Identify key risks and consequences to critical services.
- Provide assurance to government, as appropriate.

6.5.2.4 Cyber Security Response Coordination Unit (part of the National Office of Cyber Security)

- Support Victorian Government to manage consequences that may impact other jurisdictions.

6.6 WoVG Control Team or Consequence Coordination Team

6.6.1 Summary

The WoVG Control Team is activated for incidents where there is a need to direct a WoVG technical response to an incident across agencies. It provides strategic advice for incident readiness, control and relief. It also manages the integration of relief and recovery by supporting control functions and responsibilities.

The WoVG Consequence Coordination Team is activated for incidents where effective coordination across agencies is required to mitigate harms arising from the impacts and consequences of cyber incidents.

Both the WoVG Control Team and WoVG Consequence Coordination Team may operate on a formal or informal basis.

6.6.2 Roles and responsibilities

Table 6 outlines WoVG Control or Consequence Coordination Team membership. Both Teams may operate with a smaller membership if greater sensitivity is needed for the particular incident.

6.6.2.1 Department of Government Services

- Determine whether to activate the WoVG Control Team or WoVG Consequence Coordination Team.
- Determine their appropriate membership, if activated.
- Chair the WoVG Control Team and/or WoVG Consequence Coordination Team, when activated.

6.6.2.2 Impacted department or government agency

- Participate in the WoVG Control Team and/or WoVG Consequence Coordination Team on request, when activated.

TABLE 6: WoVG Control or Consequence Coordination Team membership

Severity level	WoVG category	Potential WoVG Control Team membership	Potential WoVG Consequence Coordination Team membership
1	Event	Departments and government agencies should use their own internal cyber security incident response plan for equivalent arrangements	
2	Minor		
3	**Limited**	→ DGS (WoVG Control Team Chair) → Victorian Government CISO (optional) → incident manager of the impacted department or government agency → a member of each key support agency → others as determined by the Chair	→ DGS (WoVG Consequence Coordination Team Chair) → a member of each impacted department or government agency → a member of each key support agency → others as determined by the Chair
4	**Major**	→ DGS (WoVG Control Team Chair) → Victorian Government CISO → incident manager of the impacted department or government agency → a senior member of each key support agency → others as determined by the Chair	→ DGS (WoVG Consequence Coordination Team Chair) → a senior member of each impacted department or government agency → a senior member of each key support agency → others as determined by the Chair
5	**Critical**		
6	Emergency	See the Sub-Plan for the equivalent State Control Team	See the Sub-Plan

6.7 Control or coordination centre

6.7.1 Summary

Cyber security incident control and coordination is most likely to be conducted in virtual teams. Consideration should be given to activating a particular location as a control or coordination centre to ensure an effective response if online systems are impacted by the incident.

6.7.2 Roles and responsibilities

6.7.2.1 Department of Government Services

- Determine if the response needs to be conducted from a particular physical location.

6.7.2.2 Departments and government agencies

- Attend any control or coordination centre that is activated, when required for particular activities (such as an in-person meeting).

6.8 Media and public communication

6.8.1 Summary

The community must be educated about cyber safety so they can recover quickly when impacted by a cyber security incident.

To ensure as much consistency as possible in WoVG cyber security arrangements, the Victorian Government adopts the State Emergency Management Priorities at both incident and emergency level. This includes the priority: 'issuing of community information and community warnings detailing incident information that is timely, relevant and tailored to assist community members to make informed decisions about their safety' (see **Appendix D**).

When needed, media and public communication should explain:

- the nature and impact of the cyber security incident
- the extent of affected systems, services or information
- the steps the government is taking to resolve the incident
- when systems or services are expected to return to normal (if known)
- any other information for individuals to minimise the harm of the cyber incident.

Not all incidents require media and public communication.

6.8.2 Roles and responsibilities

6.8.2.1 Nominated spokespeople

The nominated spokesperson for a cyber security incident will vary. Who speaks on the incident to the media will depend on:

- what happened
- the consequences of the incident
- current media coverage
- other incidents happening simultaneously.

The spokesperson may be the Victorian Government CISO or another government spokesperson with knowledge of the incident and/or consequences.

6.8.2.2 Impacted department or government agency, or department or government agency with a consequence

- Develop and coordinate media and public communication in consultation with DGS.
- Manage its own media and public communication channels.
- Assess the risk of harm and consider notifying affected Victorians to minimise harm.[23]
- Consult with the Victorian Managed Insurance Authority or other insurance provider about how to communicate to the public, as this could impact a future insurance claim.

6.8.2.3 Department of Government Services

- Authorise all public communication.
- Liaise with the ACSC and members of the NCSC (via the CIRS manager's presence on the NOSC) to share key messages that support consistent media and public communication across jurisdictions.
- Support departments and government agencies to develop communication and engagement plans, including providing relevant communication assets.
- Coordinate media and public communication with other departments and government agencies to support consistent messaging across WoVG.
- Work alongside the impacted department, agency or private sector organisation to provide media and public communication management for the WoVG.[24]
- Provide the DGS Secretary and Minister for Government Services with up-to-date information about the incident, where needed.

23 Refer to OVIC's guide to Managing the Privacy Impacts of a Data Breach.
24 If the impacts of the incident are isolated to a specific industry or sector, responsibility for managing media and public communication may be transferred to the relevant portfolio department or agencies.

6.9 Managing concurrent cyber security incidents

6.9.1 Summary

Multiple, unrelated cyber security incidents or emergencies can occur at the same time. Victoria's risk landscape also means that cyber security incidents may happen at the same time as other non-cyber security incidents or emergencies.

6.9.2 Roles and responsibilities

6.9.2.4 Departments and government agencies

→ Source any additional resources to respond to the incident, where CIRS has used a scaled response model and the department or government agency requires further resources. These other sources should be outlined in the department or government agency's internal incident response plan.

6.9.2.5 Cyber Incident Response Service

→ Use a scaled response model to prioritise Victorian Government resources to emergencies, then critical cyber security incidents, followed by major cyber security incidents, then limited cyber security incidents.

6.10 Controlling Victoria's consequences of a national cyber incident or emergency

6.10.1 Summary

When a national cyber security incident is declared, as outlined in the Cyber Incident Management Arrangements for Australian Governments (CIMA), and arrangements are made to coordinate a national response, this happens alongside – and does not replace – Victoria's own state-based classification and response to any incident.

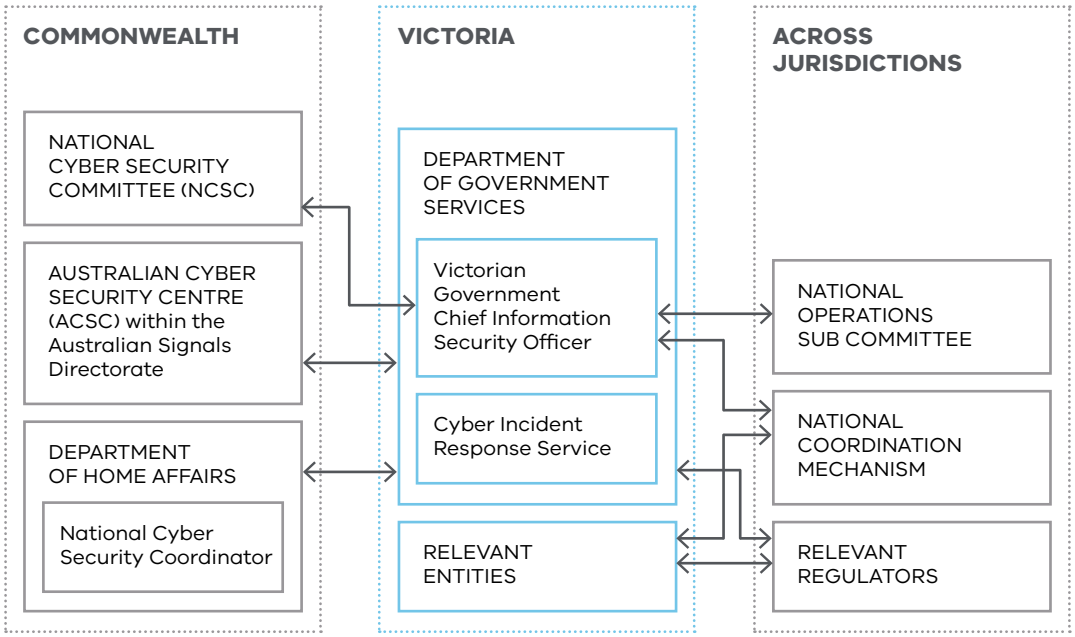
In the event of a national cyber incident, the WoVG arrangements outlined in this plan will manage the response in Victoria. This section relates specifically to the interactions between the state and the Commonwealth and across jurisdictions.

National cyber security incidents significantly impact, or have the potential to significantly impact, multiple Australian jurisdictions. Therefore they require a coordinated inter-jurisdictional response.

Contained in the CIMA are roles and responsibilities for the following stakeholders in the event of a national cyber security incident:

- state and territory governments and their law enforcement agencies
- the Commonwealth Government, including the:
  - NCSC
  - ACSC
  - National Cyber Security Coordinator
  - Department of Home Affairs – National Emergency Management Agency (NEMA)
  - Department of Prime Minister and Cabinet
  - Australian Federal Police
  - National Cyber Security Coordinator
- businesses
- the community.

FIGURE 6: Intra-jurisdictional coordination in a national cyber security incident.



6.10.2 Roles and responsibilities

6.10.2.1 Department of Government Services

- Act as the lead agency for Victoria.
- Use the Cyber Incident Management Arrangements to support Victorian Government to coordinate response activities with other jurisdictions.
- Collaborate with the relevant bodies to support an integrated operational response where state or Commonwealth coordination arrangements exist for specific industries or sectors (such as the national energy sector cyber security arrangements). This includes collaborating with the relevant Victorian Government portfolio department.

- Identify Victorian impacts and consequences in consultation with the Commonwealth Government, the ACSC, Victoria Police and emergency management agencies.
- Determine the Victorian impacts and consequences of a national emergency in accordance with this plan.
- Remain responsible for operational management (alongside broader Victorian Government departments and government agencies) of any cyber security incident within Victoria.

6.10.2.2 Victorian Government Chief Information Security Officer

- Determine the Victorian categorisation and response to a national incident.
- Represent Victoria on the NCSC.

6.10.2.3 Australian Cyber Security Centre

- Consult with cyber security leaders from affected Australian governments through the NCSC.
- Declare a national cyber incident if a cyber incident impacts, or has the potential to significantly impact, multiple Australian jurisdictions and/or requires a coordinated inter-jurisdictional response.

6.10.2.4 National Cyber Security Committee[25]

- On declaring a national cyber security incident, the NCSC will activate. It is responsible for:
  - supporting national coordination and increased situational awareness during national cyber incidents, via the Cyber Incident Management Arrangements for Australian Governments
  - supporting better situational awareness during national cyber security incidents and the coordination of response efforts
  - facilitating the exchange of information (e.g., threat intelligence and possible solutions to improve situational awareness and response)
  - facilitating the creation of nationally consistent public information
  - assisting members to consult before briefing ministers and other senior stakeholders
  - facilitating the pooling of expertise and resources.

6.10.2.5 National Office of Cyber Security

- Support cyber resilience to and recovery from nationally significant major cyber security incidents.

6.10.2.6 National Cyber Security Coordinator

- Bring together expertise and resources from across government and security agencies to ensure coordinated preparation for, and management of, consequences.

6.10.2.7 National Emergency Management Agency

- Convene the Australian Government Crisis and Recovery Committee to bring together government agencies across Australia.
- Convene the National Coordination Mechanism, as needed.

25 The NCSC is the peak cyber security coordination body for Australian governments. It includes cyber security leaders from all Australian states and territories and the Commonwealth Government.

7 Cyber security incident recovery

Recovery is how a system or service is returned to its proper level of functioning after a cyber security incident.

7.1 Summary

Aspects of the recovery phase, such as planning, can occur at the same time as the response phase. Depending on the incident, recovery activities may include ongoing consequence management.[26]

Incidents could have direct or indirect impacts across these identified 'recovery environments':

- social
- economic
- built
- natural
- Aboriginal culture and healing.

While response and recovery efforts are occurring, it is possible that the consequences cascade into another discrete non-cyber security incident or emergency type. These consequential incidents or emergencies are managed in accordance with their own arrangements.

26 Adapted from the SEMP.

7.2 Social recovery

Cyber incidents may have adverse impacts on health, wellbeing and community cohesion. Individuals and communities may experience:

- minor injuries or illness[27]
- impacted psychosocial health
- increased strain on the health system
- difficulty making decisions without clear information
- concerns about returning to 'normal' life
- disruptions to cultural practices.

A cyber security incident may impact community cohesion, leading to social division in the form of public protests, violence and mistrust of government.

7.3 Economic recovery

Cyber security incidents can negatively impact local economies. This can include a loss of business, the loss of livelihoods, as well as disruptions to the supply chain and unique shifts in demand. All hardships experienced by business owners must be considered as part of the recovery effort.

Initially, economic recovery focuses on short-term financial viability. The long-term aim is to help businesses build back up. At the core of this form of recovery are existing economic strengths and opportunities, such as the tourism industry and primary producers. Recovery also includes opportunities for small businesses, medium and large businesses, industry partners and sector leaders.

7.4 Built recovery

Cyber security incidents can impact essential utilities, services and built infrastructure. This includes water and wastewater services, electricity, telecommunications, transport and banking.

A cyber security incident could also impact significant state-owned assets, such as schools, health services, critical infrastructure and emergency management. Their cyber infrastructure would require repair and restoration following an incident.

27 More significant injuries or illness, including death, are likely to be considered as a cyber security emergency, which is addressed under the Sub-Plan.

7.5 Natural recovery

A cyber security incident may include consequences such as impact to the natural environment either directly or, more likely, indirectly.

7.6 Aboriginal culture and healing

Cyber security incidents can impact Victoria's First Peoples. Negative consequences include:

- disruption of service provision through Aboriginal community-controlled organisations and Traditional Owner corporations
- loss of data sovereignty
- theft of sensitive cultural heritage information and traditional knowledge
- delays in critical care
- impacts on land and resource management
- adverse health impacts.

Victoria's First Peoples may also be a target for cybercrime. This can result in disinformation, phishing attacks and harassment relating to communities, culture or land rights.

7.7 Roles and responsibilities

7.7.1 Impacted department or government agency

- Responsible for the restoration and recovery of own cyber security incident affected infrastructure.
- Implement disaster recovery arrangements to return impacted systems and services to normal operation as soon as possible.
- Liaise with Victorian Managed Insurance Authority or other insurance provider to determine what support for recovery is available.
- Prepare a recovery plan in a manner that reflects the type and severity of incident. It should be prepared in conjunction with advisers in business continuity and IT services. It should detail:
  - the approach to recovering IT networks, systems and applications once containment and eradication is complete
  - a plan to restore systems to normal operation
  - a process of continual monitoring to confirm that the affected systems are functioning normally
  - a plan to prevent similar incidents occurring (if applicable).

This recovery plan may also include a related criminal investigation (including forensic evidence collection). This investigation may need to be complete before recovery is possible.

- Test systems/services to ensure the threat has been eradicated and affected systems/services are back to normal function.
- Determine any stakeholder communication requirements.
- Establish monitoring for impacted natural and cultural heritage values, in consultation with all affected communities, including Victoria's First Peoples and Traditional Owner groups.
- Provide DGS with updates on recovery progress. This may include activities around lessons learned, which inform cyber security incident continuous improvement processes.

7.7.2 Portfolio department or government agency

- Lead recovery activities with support agencies.
- Consider the impacts on recovery environments.

7.7.3 Department of Government Services

- Provide a peer review of any advice provided to the impacted department or government agency by a contracted service provider. DGS does not approve, endorse or provide assurance of these products.

7.8 Closing out an incident

7.8.1 Summary

The decision to stand down a WoVG response to an incident is made by the DGS in consultation with the impacted department or government agency.

7.8.2 Roles and responsibilities

7.8.2.8 Department of Government Services

- Advise the closure of the WoVG response following consultation with the impacted department or government agency.
- Provide the impacted department or government agency with a report outlining activities, finding and recommendations, if CIRS has been involved in forensic investigation.

7.8.2.9 Impacted department or government agency

- Continue its internal recovery in line with its own recovery plan and with consideration to any report provided by CIRS, while the WoVG response is closed.

8 Lessons and evaluation

8.1.1 Summary

Evaluation helps to improve responses to future incidents. Reviews should identify what was effective and what can be improved.

8.1.2 Roles and responsibilities

8.1.2.1 Impacted department or government agency

- Conduct a debrief or review to document learnings from the mitigation, response and recovery activities. This review should analyse the root cause and any remaining vulnerabilities, as well as identify what was most effective and what can be improved.
- Gather copies of all notes taken during the response to assist with lessons and evaluation.
- Share outcomes from the review with a wide range of stakeholders, including DGS.
- Consider review outcomes in the next review of the cyber security incident response plan to reflect better practice.
- Develop an action plan with sustained, new or modified activities to address the identified areas for improvement and prevent future incidents.
- Monitor implementation of relevant actions arising from the review.

8.1.2.2 Department of Government Services

- Where the incident has required significant investment from DGS, it should:
  - document and monitor learnings from response and recovery activities related to DGS' involvement
  - share outcomes from the review for relevant stakeholders to utilise identified lessons
  - assess identified lessons for change/improvement activities
  - consider review outcomes in the next review of this Plan to reflect better practice.

9 Appendices

Appendix A Acronyms

TABLE 7: List of acronyms

Acronym	Original
ACSC	The Australian Signals Directorate's Australian Cyber Security Centre
AGCMF	Australian Government Crisis Management Framework
AIIMS	Australasian Inter-Service Incident Management System
ASD	Australian Signals Directorate
BCP	Business Continuity Plan
BIL	Business Impact Level
CCT	Consequence Coordination Team
CI	Critical Infrastructure
CT	Control Team
CISC	Department of Home Affairs' Cyber and Infrastructure Security Centre
CIMA	Cyber Incident Management Arrangements for Australian Governments
CIRS	Department of Government Services' Cyber Incident Response Service
CISO	Chief Information Security Officer
CSIMP	Cyber Security Incident Management Plan (this plan)

Acronym	Original
DF	Digital Forensics
DGS	Department of Government Services
DHA	Department of Home Affairs
DoS/DDoS	Denial of Service/Distributed Denial of Service
DR	Disaster Recovery
E8	ACSC's Essential Eight Maturity Model
EMC	Emergency Management Commissioner
EM Act 2013	*Emergency Management Act 2013* (Vic)
EM Act 1986	*Emergency Management Act 1986* (Vic)
EMV	Emergency Management Victoria
IC	Incident Controller
IMT	Incident Management Team
IR	Incident Response
IP	Internet Protocol
IRAP	Information Security Registered Assessors Program
ISM	Australian Government Information Security Manual
MSP	Managed Service Provider
NCM	National Coordination Mechanism
NCSC	National Cyber Security Committee
NEMA	National Emergency Management Agency
NIST	National Institute of Standards and Technology
NOSC	National Operations Sub-Committee
NOCS	National Office of Cyber Security, part of the Department of Home Affairs
OVIC	Office of the Victorian Information Commissioner
PDP Act	*Privacy and Data Protection Act 2014* (Vic)
PIO	Public Information Officer
PSPF	Protective Security Policy Framework

Acronym	Original
SCRC	State Crisis and Resilience Council
SEMP	State Emergency Management Plan
SITREP	Situation Report
SOC	Security Operations Centre
SOCI Act	*Security of Critical Infrastructure Act 2018* (Cth)
SOP	Standard Operating Procedure
SRN	Sector Resilience Network
justPortal	Whole of Victorian Government Cyber Security Portal
TLP	Traffic Light Protocol
VERA	Victorian Emergency Risk Assessment
VGRMF	Victorian Government Risk Management Framework
Victorian Government	Victorian Government
VicGov	Victorian Government
VicPol	Victoria Police
VMIA	Victorian Managed Insurance Authority
VPDSF/S	Victorian Protective Data Security Framework/Standards
VPF	Victorian Preparedness Framework
WoVG	Whole of Victorian Government

Appendix B

Common sources of cyber security compromise or consequence

TABLE 8: Summary of common sources of cyber security compromise or consequence

Type	Description	Suggested initial response to minimise potential harm
Ransomware	A tool used to encrypt or lock victims' data until a ransom is paid.	Immediately remove the infected device/s from the network to limit the spread of ransomware. Capture all available logs relevant to the device. Isolate the devices while containment and eradication activities are determined.
Malware infections	A code-based malicious entity that successfully infects a host (such as virus, worm or trojan horse).	Immediately remove the infected device/s from the network to limit the spread of malware. Capture all available logs relevant to the device. Isolate the devices while containment activities are confirmed and eradication efforts are determined.
Denial of Service (DoS) /Distributed Denial of Service (DDoS) attacks	Overwhelming a network with traffic that it cannot process, sometimes causing the network to fail.	Request gateway services provider to identify DoS/DDoS nature, attack vector and implement suitable solutions. Liaise with gateway services and network team to apply filters at network edge and/or increase capacity.
Phishing and social engineering	Deceptive communication designed to elicit users' sensitive information (including network credentials).	Review logs of affected users (web and email logs) to determine whether malicious links/attachments were accessed. Consult users to confirm what actions they took and whether any personal/sensitive information was provided in response to a phishing/social engineering attempt. Consider resetting user passwords and monitoring accounts for any unauthorised access.
Data breach	Unauthorised access to sensitive or personally identifiable information (including public sector data).	Contain the data loss/spill as soon as possible. Alert privacy, legal and communication/media teams. Investigate the cause of the data loss/spill. For more information, refer to the OVICs Managing the Privacy Impacts of a Data Breach.

Appendix C

Comparison of Whole of Victorian Government cyber security incident categories with Business Impact Levels

The Whole of Victorian Government (WoVG) cyber incident categories are prepared as a comparable state-level equivalent to the Office of the Victorian Information Commissioner's (OVIC's) entity-level Business Impact Levels (BILs).[28]

OVIC is the primary regulator and source of independent advice to the community and Victorian Government about how the public sector collects, uses and discloses information.

WoVG categories are similar to an internal department or government agency cyber incident but at a state-scale. Importantly, the 2 sets of categories do not otherwise match up with each other. For example, an entity may identify a BIL 4 'Serious' incident. While treated seriously by the department or government agency, it does not equate to a cyber security emergency at the state level.

TABLE 9: Comparison between WoVG incident categories and BILs

For use at a WoVG scale		**For use internally within a department or government agency[29]**	
Severity level	WoVG category	Business impact	BIL
1	Cyber security event	N/A	BIL 0
2	Minor cyber security incident	Minor	BIL 1
3	Limited cyber security threat or incident	Limited	BIL 2
4	Major cyber security threat or incident	Major	BIL 3
5	Critical cyber security incident		
6	Cyber security emergency	Serious	BIL 4
		Exceptional	BIL 5

28 VPDSF BILs, Version 2.1, November 2019.
29 While the requirements surrounding BILs of the VPDSF are not applicable to councils (except in some instances where the council may act as Committee of Management for Crown Land Reserves), councils may optionally consider BILs in their own cyber security arrangements.

Appendix D

State Emergency Management Priorities

The State Emergency Management Priorities are extracted from the State Emergency Management Plan (SEMP).

TABLE 10: Summary of relevant State Emergency Management Priorities

State Emergency Management Priorities
Protection and preservation of life and relief of suffering is paramount. This includes: → Safety of emergency response personnel; and → Safety of community members including those most-at-risk in emergencies, residents, and visitors/tourists.
Issuing of community information and community warnings detailing incident information that is timely, relevant and tailored to assist community members make informed decisions about their safety.
Protection of critical infrastructure and community assets that support community resilience.
Protection of residential property as a place of primary residence.
Protection of assets supporting individual livelihoods and economic production that supports individual and community financial sustainability.
Protection of environmental and conservation assets that considers the cultural, biodiversity and social values of the environment.

Appendix E
Sector Resilience Networks

Sector Resilience Networks (SRNs) are a key link between business and the Victorian Government. They bring critical infrastructure sectors together under Victoria's Critical Infrastructure Resilience Strategy.

Sector Resilience Networks

→ Provide a forum for business and government to discuss sector challenges, dependencies, opportunities and best practice, as required by responsible government departments.

TABLE 11: Overview of SRNs

SRN	Responsible portfolio department	Responsible portfolio department
1	Water	Department of Energy, Environment and Climate Action
2	Transport	Department of Transport and Planning
3	Energy	Department of Energy, Environment and Climate Action
4	Food supply and grocery	Department of Jobs, Skills, Industry and Regions
5	Banking and finance	Department of Treasury and Finance
6	Government	Department of Premier and Cabinet
7	Telecommunications	Department of Government Services
8	Health	Department of Health

Department of Government Services

→ Work with various SRNs or equivalent key stakeholder groups to provide critical infrastructure owners and operators with advice on cyber security emergency risks and mitigation strategies.

Emergency Management Victoria

→ Chair the Critical Infrastructure Resilience Sectors Forum. This forum's members include the Chairs of each SRN.

Appendix F

Frameworks for cyber security maturity

Australian Cyber Security Centre's 'Essential Eight' maturity model

The Australian Cyber Security Centre (ACSC) has developed Strategies to Mitigate Cyber Security Incidents. These are prioritised mitigation strategies. These help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies is the 'Essential Eight' (E8). The model outlines 3 levels of maturity for each of the 8 categories:

- Application control
- Patch applications
- Configure Microsoft Office macro settings
- User application hardening
- Restrict administrative privileges
- Patch operating systems
- Multi-factor authentication
- Regular backups

The E8 strategies protect Microsoft Windows-based internet-connected networks.

No single mitigation strategy can prevent cyber security incidents. However, the E8 when used to its full potential, is so effective at mitigating targeted cyber intrusions that the ACSC considers this the cyber security baseline for all entities.

For entities that use the Information Security Manual (ISM), the ACSC provides mapping between the E8 and the security controls contained in the ISM.

Cyber Security Framework, National Institute of Standards and Technology (NIST; USA)

The NIST Cyber Security Framework provides a comprehensive approach to improving cyber maturity, including alignment to the E8, while meeting obligations within the VPDSF/S.

The NIST Cyber Security Framework is aligned to ISO27001 and integrates industry standards and best practices to help organisations manage their cyber security risks.

This framework provides a set of cyber security activities, desired outcomes and applicable references that are common across critical infrastructure sectors. It provides a common language to develop a shared understanding of sector specific cyber security risks.

This framework can be used by organisations that already have extensive cyber security programs, as well as those just beginning to think about putting cyber security management programs in place.

This framework not only helps organisations understand their cyber security risks (threats, vulnerabilities and impacts), but also how to reduce these risks with customised measures.

This framework also helps organisations respond to, and recover from, cyber security incidents, prompting them to analyse root causes and consider how they can make improvements.

Protective Security Policy Framework

The Protective Security Policy Framework (PSPF) helps Commonwealth Government entities to protect their people, information and assets, both at home and overseas.

It sets out the Australian Government's protective security policy and supports entities to effectively implement this policy across:

- security governance
- information security
- personnel security
- physical security.

Victorian Government Risk Management Framework

The Victorian Government Risk Management Framework (VGRMF), published by the Department of Treasury and Finance, applies to departments and public bodies covered by the *Financial Management Act 1994* (Vic).

This framework describes the minimum risk management requirements agencies must meet to demonstrate that they are managing risk effectively, including shared and state significant risk.

Victorian Protective Data Security Framework and Standards

Published by Office of the Victorian Information Commissioner (OVIC), this is Victoria's overall scheme for managing protective data security risks in Victoria's public sector.

It also consists of the:

- assurance model
- supplementary security guides and supporting resources.

The Victorian Protective Data Security Standards establish 12 high-level mandatory requirements to protect public sector information across all security areas:

1. Information Security Management Framework
2. Information Security Value
3. Information Security Risk Management
4. Information Access
5. Information Security Obligations
6. Information Security Incident Management
7. Information Security Aspects of Business Continuity and Disaster Recovery
8. Third Party Arrangements
9. Information Security Reporting to OVIC
10. Personnel Security
11. ICT Security
12. Physical Security

Australian Energy Sector Cyber Security Framework

The Australian Energy Sector Cyber Security Framework has been developed through collaboration with industry and government stakeholders, including the Australian Energy Market Operator, ACSC, CISC and representatives from Australian energy organisations.

This framework leverages recognised industry frameworks such as the US Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model and the NIST Cyber Security Framework and references global best practice control standards (such as ISO/IEC 27001).

This framework also incorporates Australian-specific control references, such as the E8 strategies, the Australian Privacy Principles and the Notifiable Data Breaches scheme.

Appendix G

Summary of threat intelligence products

TABLE 12: Summary of threat intelligence products

Product	Summary	Audience
Alert	→ Provides practical and technical intelligence with actionable information which requires urgent action and attention. → Is prepared in response to or to provide a warning about an issue, vulnerability or threat campaign.	→ IT practitioners
Advisory	→ Highlights areas for situational awareness, monitoring and consideration. → Is prepared in response to, or to provide a warning about, an issue, vulnerability or threat campaign. → Can contain practical and actionable information, as needed.	→ IT practitioners
Intelligence brief	→ Provides analysis of a trend, issue or problem with potential WoVG impacts.	→ IT practitioners
Intelligence summary	→ Gives an overview of intelligence and actions taking place during an ongoing incident. → Is prepared when an issue becomes larger in scope (for example, has a multi-agency impact).	→ Cyber leads → Executives → Communications → Management
Situational report	→ Provides regular updates on a specific risk, issue or incident. → Is prepared to inform a common understanding of a situation, including details of current priorities and future actions.	→ Cyber leads → Executives → Communications → Management

Appendix H

Contact details of key stakeholder agencies

TABLE 13: Contact details of key stakeholder agencies

Key Stakeholder	Phone	Emails (monitored during business hours)	Website
Australian Cyber Security Centre (ACSC)	**1300 CYBER1** (1300 292 371) Monitored 24/7	asd.assist@**defence**.gov.au	www.cyber.gov.au/report-and-recover/report
Department of Government Services' Cyber Incident Response Service (CIRS)	**The Whole of Victorian Government Cyber Security Portal is the preferred method for notification**		
	1300 278 842	cybersecurity@**dpc**.vic.gov.au This email is likely to be updated to cybersecurity@**dgs**.vic.gov.au before this plan is updated again.	Whole of Victorian Government Cyber Security Portal **(preferred method for notification)** vicgov.sharepoint.com/sites/VG002650/SitePages/Incident-Reporting.aspx
National Office of Cyber Security (NOCS)	–	General enquiries: cscsupport@**homeaffairs**.gov.au Consequence management enquiries: Cyber Security Response Coordination Unit, csrcu@**homeaffairs**.gov.au	www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/cyber-coordinator
Office of the Victorian Information Commissioner (OVIC)	**1300 00 OVIC** (1300 006 842) Monitored 9am-5pm, Monday to Friday	incidents@**ovic**.vic.gov.au	www.ovic.vic.gov.au/privacy/resources-for-organisations/information-security-and-privacy-incident-notification-form
Victorian Managed Insurance Authority (VMIA)	**03 9270 6900** Monitored 9am-5pm, Monday to Friday **1300 135 790** For after hours enquiries	claims@**vmia**.vic.gov.au	www.vmia.vic.gov.au
Victoria Police (VicPol)	If there is a threat to life or risk of harm, call **000**	–	www.police.vic.gov.au/report-cybercrime

Appendix I

Summary of Australasian Inter-Service Incident Management System functions

In line with the State Emergency Management Plan (SEMP), the Victorian emergency management sector operates under the Australasian Inter-Service Incident Management System (AIIMS).

Smaller incidents may be manageable without formal activation of an Incident Management Team (IMT).

The DGS Incident Controller (IC) will create and oversee an IMT if they believe a team is needed to manage the response. The DGS IC may delegate functions to others. The structure of each IMT is tailored to the nature and severity of the incident.

FIGURE 7. Diagram showing the hierarchy and function of the AIIMS

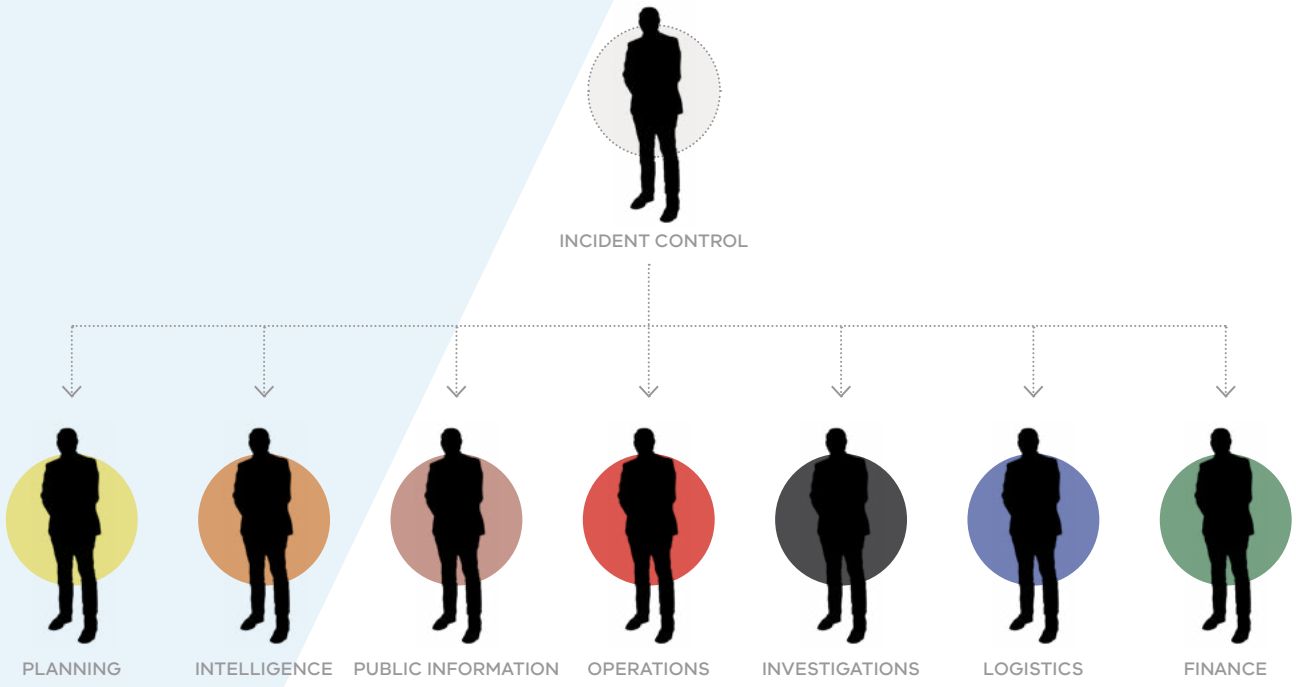


TABLE 14: Summary of AIIMS

Function	Description
Control	Management of all activities necessary to resolve an incident.
Planning	Development of objectives, strategies and plans to resolve an incident based on information collected and analysed.
Intelligence	Collection and analysis of information or data, to be recorded and shared as intelligence to support decision-making and planning.
Public information	Provision of warnings, information and advice to the public. Liaison with the media and affected communities.
Operations	Tasking of roles and application of resources to resolve the incident.
Investigation	Determination of the cause of an incident and/or factors that contributed.
Logistics	Acquisition and provision of human and physical resources, facilities, services and materials to achieve incident objectives.
Finance	Management of: → accounts for purchases of supplies and hire of equipment → insurance and compensation for personnel, property and vehicles → cost data collection and provision of cost-effectiveness analyses → cost estimates for the incident.
Lessons and evaluation[30]	Collection and analysis of observations and activities. Monitoring the progress of implementation of improvement activities.

30 This is an additional function added in recognition of its importance in establishing a culture of continuous improvement in Victoria. It is not a recognised AIIMS function.

DGC Transformation Projects 240902

VICTORIA State Government | Government Services