Control Agency for Cyber Crisis

Incident Management Framework

Government of South Australia

TABLE OF CONTENTS

1 INTRODUCTION

Incidents affecting telecommunications, and information technology can occur every day and emanate from a range of sources, impacting governments, organisations as well as the community. As our reliance on information and communications technology has grown, so too has the need for incidents to be effectively managed as part of a structured security and response framework. The Government of South Australia's approach is to handle these incidents through the State's emergency management arrangements as outlined under the Emergency Management Act 2004 (the Act) and the State Emergency Management Plan (SEMP).

The Act and SEMP identifies the Department of the Premier and Cabinet (DPC) as the Control Agency for Cyber Crisis (formerly Control Agency for ICT Failure) to lead a coordinated response to prepare for, respond to, and recover from cyber security and telecommunication incidents affecting government or the community. In this context, a Cyber Crisis is malicious cyber activity and or telecommunications disruption with consequences so severe the South Australian Government Cyber Crisis Management Framework is activated, and an incident management team is appointed to coordinate the response.

This Framework outlines how DPC fulfils its responsibilities as the Control Agency for Cyber Crisis, including the roles, responsibilities and actions to prepare for, respond to, and recover from an emergency. While the emphasis of this Framework is the role of DPC in incident management, it is acknowledged that an effective response requires a collaborative approach involving a range of stakeholders from across all sectors.

This Framework forms part of a suite of documents which outline the emergency management and incident management activities performed by DPC and coordinated by the Office for Cyber Security.

Cyber security and increasing resilience of critical systems, including telecommunications, is a major focus of the Department of the Premier and Cabinet (DPC) and the Government of South Australia, as outlined in the South Australian Cyber Security Strategic Plan 2018-2021.

Chief Executive
Department of the Premier and Cabinet

State Controller – Control Agency Cyber Crisis
Executive Director, ICT & Digital Government
Department of the Premier and Cabinet

2 DOCUMENT DESCRIPTION

2.2 Document Purpose

The purpose of this document (the Framework) is to outline how DPC, under the coordination of the Office for Cyber Security, will fulfil its responsibilities as the Control Agency for Cyber Crisis.

2.3 Objective

The objective of this Framework is to outline the arrangements for ensuring a comprehensive approach to the state's management of cyber security and telecommunication emergencies, which aligns with the state's emergency management arrangements.

2.4 Audience

This Framework is prepared for all key private and public-sector stakeholders of the Control Agency for Cyber Crisis.

No plan can ever completely cover all contingencies. DPC staff must exercise judgement and use flexibility when confronted with the various emergency situations or incidents.

The arrangements detailed in this Framework aim to complement the incident management activities already performed by individual agencies and organisations. This Framework and its supporting documents do not remove the need for agencies to have their own incident management capability. Agencies should refer to ISMF 'Policy Statement 12' for more information about their own incident management responsibilities.

2.5 Authority

This Framework is prepared for DPC by the Office for Cyber Security, under the leadership of the Executive Director, ICT and Digital Government and the South Australian Government Chief Information Security Officer (CISO).

Emergency Services and other agencies in South Australia are assigned significant and specific responsibility in legislation and the emergency management arrangements. For each emergency there is only one control authority (i.e. Control Agency) responsible for resolving that emergency. Authority for control carries with it responsibility for tasking and coordinating other organisations in accordance with the needs of a situation. Authority includes:

- The SEMP, formed under Section 9 (1) (b) of the Act, identifies DPC as the Control Agency for 'Cyber Crisis'.
- State and Deputy State Controllers of the Control Agency for Cyber Crisis are appointed 'Authorised Officers' under the *Emergency Management Act 2004.*

  State and Deputy State Controllers may also direct workers of a government agency to conduct in a particular manner, specific to the containment/response to incidents, in accordance with the requirements of *Cabinet Circular PC042- Cyber Security Incident Management.*

2.6 Responsibility

In accordance with the Common Incident Management Framework for all Control Agencies, DPC must take a functional management approach that aligns with the ten responsibilities (**Table 1**) of a Control Agency.

Table 1: The ten responsibilities of a Control Agency

Functions	Responsibilities of a Control Agency
Command and Control	Take control of the response to the emergency (including the appointment of an incident controller and management structure)
Safety	Ensure a safe working environment and safe systems of work
Communication	Ensure effective liaison, communication and cooperation with all involved
Intelligence	Continually assess the situation, identify risks and share information with all involved
Planning	Develop and share plans and strategies that meet the requirements of all persons and agencies responding to the emergency (incident action plan)
Operations	Implement and monitor an incident action plan
Logistics	Ensure the effective allocation and use of available resources
Public Information	Ensure the public is adequately informed and warned so as to enhance community resilience
Investigation	Facilitate the investigation of the emergency and review of response activities
Recovery	Ensure transition from response to recovery including the coordinated handover to the state recovery arrangements

2.7 Document History

The Cyber Crisis Incident Management Framework will be reviewed on a by annual basis or as required. Version v4.0 supersedes all previous versions including:

- ICT Incident Management Framework version 1.0
- ICT Incident Management Framework version 2.0
- ICT Incident Management Framework version 3.0

2.8 Document Hierarchy

The following provides an overview of the of the key relevant incident and emergency management documents:

- South Australian State Emergency Management Plan: The SEMP sets out the state's comprehensive emergency management arrangements.
- Cyber Crisis Incident Management Framework (this document): Outlines key roles, responsibilities and actions to prepare for, respond to, and recover from a Cyber Crisis.
- Cyber Security Incident Response Plan: This plan has been developed to assist the Control Agency for Cyber Crisis to respond to reports of Cyber Security Events and Cyber Security Incidents
- Cyber Crisis Operations Manual: Processes & Procedures for responding to a Significant Cyber or Communications Incident.
- Cyber Crisis Response Action Cards: Identifies tasks and responsibilities, broken down into required actions that are identified in action cards.
- Cyber Crisis Communications Manual: This Communications Plan has been created to assist the Control Agency for ICT Failure's Public Information function to provide external communications, ensuring the public is adequately informed and warned to enhance community resilience.
- Cabinet Circular PC042 - Cyber Security Incident Management: Addresses the requirement for South Australian Government agencies to manage, report and respond to cyber security incidents in coordination with the Control Agency for Cyber Crisis.
- ISMF Standard 140: Establishes the requirement for South Australian Government agencies and contracted suppliers to report cyber security events and incidents.

2.9 Document Approach

The Control Agency for Cyber Crisis embraces an 'all hazards' approach to the prevention or mitigation of incidents, preparedness for their impact, response to that impact and recovery from the consequences. Much of the work the Office for Cyber Security does on a day to day basis contributes to mitigating incidents and preparing for their impact. The following sections outline the Control Agency's Prevention, Preparedness, Response and Recovery activities.

3 PREVENTION

Prevention includes the identification of hazards, the assessment of threats to life and property, and measures to reduce or eliminate potential loss to life or property and protect economic development.

3.1 South Australian Government Cyber Security Strategic Plan

The South Australian Cyber Security Strategic Plan 2018-2021 seeks to safeguard state infrastructure, digital assets and citizen information against the increasing incidence of cybercrime and espionage. This will help deliver more responsible data sharing for social change, better protect the safety and prosperity of South Australians, and enhance the government's digital engagement with the business community.

3.2 Cyber Security Toolkit

The Cyber Security Toolkit is a set of tools that the SA Government provides all government agencies, local government and large SA based private sector organisations. The toolkit involves online services specifically designed for aiding in the prevention of, and preparedness for, cyber security threats, and also aid a whole of state response to serious cyber security threats when they occur.

3.3 Intelligence, Threat & Risk Assessments

The Office for Cyber Security is involved in a range of intelligence, threat and risk assessment activities which assist in the identification and assessment of threats to assets and service delivery. This includes reviewing incidents, preparation and dissemination of weekly briefs to key stakeholders.

3.4 Information Security Standards

The Information Security Management Framework (ISMF) addresses cyber security in the Government of South Australia and consists of 40 policies supported by 140 standards. The ISMF applies to South Australian Government agencies and suppliers whose contractual requirements include it.

3.5 Across Government ICT Procurement Arrangements

Suppliers of ICT services to Government are required to comply with and promote the use of the ISMF, and all subordinate documentation. They are also required to work with DPC as part of the emergency management arrangements

3.6 State and Commonwealth Committees

DPC has representatives on the following across government emergency management governance groups:

- Emergency management Council of Cabinet (EMC)
- State Emergency Management Committee (SEMC)
- SEMC Advisory Groups
- Trusted Information Sharing Network (TISN) – Communications Sector Group
- National Cyber Security Steering Committee
- National Cyber Security Operations Capability Committee

4 PREPAREDNESS

Preparedness describes arrangements to ensure that, should an emergency/incident occur, the resources and services needed to manage the effects can be efficiently mobilised and deployed.

Being prepared is understanding the threat and the establishment of systems for the management of incidents, education and training. Preparedness and planning are undertaken before an emergency occurs.

4.1 State Emergency Management Arrangements

The SEMP outlines an 'all-hazards approach' to emergency management as a large range of hazards can cause similar problems, and similar arrangements are required to manage them. This includes key roles and responsibilities.

4.2 State Controller/ Deputy State Controller

The State Controller is responsible for the overall operation of the Control Agency and effective decision-making concerning the operational requirements during a declared emergency or disaster. The State Controller and Deputy State Controllers are Authorised Officers appointed under Section 17 of the *Emergency Management Act (2004)*, an Authorised Officer has statutory powers under this Act and will enact these upon the declaration of an identified Major Incident, Major Emergency or Disaster (s25 the Act).

There is always a 'duty' State Controller or Deputy State Controller on call that is tasked with the overarching strategic leadership of incident management operations. The on-duty State/Deputy State Controller is the escalation point for the Duty Officer.

4.3 Duty Officer

The Duty Officer is a 24/7 rostered position that provides the emergency contact point for those needing to contact the Control Agency.

The Duty Officer will escalate matters to the on duty State/Deputy State Controller as required.

4.4 Watch Desk

The Control Agency maintains a threat intelligence and cyber security function which supports incident, crisis and emergency management. This function is referred to as the Watch Desk.

4.5 Incident Controller

The responsible officer designated by the Control Agency to lead response operations during an incident.

4.6 Support Agency Incident Commander

When a Control Agency is supporting another Control Agency, its leader shall be known as the Incident Commander.

4.7 Incident Management Team

The Incident Management Team (IMT) is assembled during an incident to oversee the Control Agency response to the incident. The IMT for the Control Agency for Cyber Crisis is comprised of staff from across DPC.

4.8 Executive Liaison Officers

Executive Liaison Officers (ELO) are emergency contact points within each agency. The role acts as the primary contact for the Control Agency in an emergency. The ELO is engaged to assist, or make decisions on behalf of their organisation, during an incident.

Executive Liaison Officers are typically the Agency Security Executive (unless otherwise advised by an agency). ELO's are a requirement under Cabinet Circular PC042-Cyber Security Incident Management.

4.9 DPC Liaison Officer

The DPC Liaison Officer represents the State Controller (if delegated) at the State Emergency Centre, advising on Support Agency operations, capacity, capability and resource availability.

4.10 DPC State Emergency Centre Liaison Officer

The DPC Liaison Officer provides operational and administrative support to the State Emergency Centre DPC Liaison Officer at the SEC during an activation.

4.11 Private Sector Collaboration

During an emergency all telecommunications sector organisations feed directly through the Control Agency for Cyber Crisis State Control Centre as part of the State Emergency Management Arrangements. The State Control Centre activates in an emergency, should it be required. Information from that Centre will be fed directly in to the State Emergency Centre by the Department of the Premier and Cabinet.

The Telecommunications Sector comprises the owners and operators of critical communications infrastructure and relevant government representatives in South Australia. The Department of the Premier and Cabinet conduct an annual Forum that enables the necessary networks and relationships to be formed to assist the Control Agency for Cyber Crisis in responding to major state-wide telecommunications failures.

4.12 Public Information and Warnings

The Control Agency for Cyber Crisis has a responsibility to ensure that the public is adequately informed and warned to support community safety and promote general awareness. The Control Agency has put in place the necessary arrangements for the ABC Emergency Broadcasting to provide information to the community.

4.12.1 ABC Emergency Broadcasting

The ABC Emergency Broadcasting service delivers warnings, alerts, information and news about disasters and emergencies on AM Radio. This would be used predominately when other communications channels are unavailable.

4.13 Training & Exercising

DPC coordinates an annual training and exercise program. This program enables the development of key roles and validates plans, systems and procedures to ensure an effective response to incidents

4.14 Emergency Management Centres/Facilities

4.14.1 State Control Centre

The State Control Centre is the generic term for the nominated location used by Control/Support Agency to control the incident or command their staff. Control Agencies are required to maintain a State Control Centre used to coordinate incident response activities. The State Control Centre is maintained and managed by DPC.

4.14.2 State Emergency Centre

The State Emergency Centre (SEC), it is an entity, created by the State Emergency Management Plan, which brings together participating agencies and support staff to coordinate State level support to agencies engaged in resolving emergencies. The SEC is maintained and managed by SA Police.

5 RESPONSE

Response is action taken and measures planned in anticipation of, during, and immediately after an incident to ensure that its effects are minimised, and that stakeholders and agencies affected are given support.

5.2 Incident Management Arrangements

The Control Agency shall be the primary element of the response component in resolving an emergency (**refer Appendix 3**). All other persons and agencies involved in response operations in relation to an emergency are carrying out those operations in support of the Control Agency.

5.2.1 Common Incident Management Framework

Incident Command and Control is the method of incident management in South Australia. Control Agencies shall support this concept by adopting commonality in incident management. This common framework is designed to enhance incident management systems currently in use by agencies, for example the Australasian Interagency Incident Management System.

5.2.2 Incident Command and Control

Incident Command and Control is the method of incident management in South Australia. Control Agencies shall support this concept by adopting commonality in incident management. Functional management is applied at emergencies at all management levels – field and strategic (regional and state) management levels – and aligns with the ten responsibilities of a Control Agency as described in the SEMP.

5.3 Control Agency

The response actions that the Control Agency will take in relation to a Cyber Crisis incident are dependent on the Severity of the incident coupled with other factors that may be occurring at that time.

5.4 Cyber Crisis Operations Manual

The Operations Manual forms part of a suite of documents which outlines the emergency management and incident management responsibilities within DPC. The manual details the processes and procedure for those incidents that fall within the Cyber Crisis Incident type.

5.5 Cyber Crisis Response Action Cards

The Cyber Crisis Response Action Cards is a document that identifies tasks and responsibilities, broken down into required actions that are identified in action cards. This document is divided into incident sections, each with a specific action card position and number to define required activities

5.6 Incident Severity Categories

The response activities that the Control Agency will take in relation to a Cyber Crisis incident is dependent on the severity of the incident, and the outcome of the risk assessment. A three-tiered severity categorisation system has been adopted. The three levels are designed as a guide for Control Agency staff on the level of response activities the incident will receive **(refer Table 2).** The Duty Officer will determine the initial incident severity, escalating to the State/Deputy State Controller when a Cyber Crisis or Significant Cyber Crisis Incident categorisation is likely.

Table 2 – Incident Severity Categories

Incident Severity Level	Description	Key Factors
Cyber Security Event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant.	Not for Public Version
Cyber Security Incident	A single or series of unwanted or unexpected cyber security events with a significant probability of compromising business operations and threatening the confidentiality, integrity or availability of a system or information.	
Significant Cyber Security Incident	A single or series of unwanted or unexpected cyber incidents with a significant probability of compromising essential business operations and/or online services, threatening the security of critical information, or resulting in a loss of confidence in government. Decision making with whole of government considerations most likely required.	
Cyber Crisis	Malicious cyber activity, with consequences so severe the full Cyber Crisis Incident Management Framework is activated for a whole-of-government or whole of state response. These incidents are likely to involve intensive media coverage, place large demands on state-wide agency resources, and impact the availability of critical services. Decision making with whole of government and whole of state considerations will be required. Community impact considerations will be required.	

5.7 Telecommunications Incident Severity Categories

In an emergency in South Australia will be the coordination and contact point for all telecommunications and communications sector organisations.

This framework covers the arrangements to coordinate large scale, severe and significant disruptions to major telecommunications infrastructure resulting in the loss of telecommunications services to a widespread area. The response activities that the Control Agency will take in relation to a telecommunications incident is dependent on the severity of the incident, and the outcome of the risk assessment.

A two-tiered severity categorisation system has been adopted. The two levels are designed as a guide for Control Agency staff on the level of response activities the incident will receive **(refer Table 3).**The State/Deputy State Controller will determine the initial incident severity on the basis of an operational risk assessment and in consultation with the Duty Officer.

Table 3 – Telecommunications Incident Categories

Incident Severity Level	Description	Key Factors
Significant Telecommunications incident	An incident, or series of unwanted or unexpected incidents, affecting telecommunications infrastructure and services with a significant impact to the community and/or essential services.	Not for Public Version
Telecommunications Crisis	A communications failure, with consequences so severe the South Australian Government Cyber Crisis Management Framework is activated. These incidents are likely to involve intensive media coverage, place large demands on state-wide agency resources, and impact the availability of critical services. Decision making with whole of government and whole of state considerations will be required. Community impact considerations will be required.	Not for Public Version

5.8 Incident Escalation

Regardless of the type of incident (i.e. Cyber Crisis or Telecommunications), the decision to escalate from one level of incident severity to the next is made by the State or Deputy State Controller. The State or Deputy Controller will consider a range of factors when making this determination (refer to the State Controller Guideline) and should use an operational risk assessment as part of this process.

5.9 Operational Risk Assessment

Operational risk assessments will be carried out as required. These assessments will aid the Duty Officer and Deputy State Controller to determine:

- Major risks and impacts
- Severity Level & Response Level

5.10 Support Agency

Where a Control Agency is not the lead for a particular emergency, they will be referred to as a Support Agency. A Support Agency will support the nominated Control Agency and is subject to direction by the nominated Control Agency. A Support Agency will have their own Incident Management Team (**refer Appendix 4**).

As a Support Agency, the Control Agency for Cyber Crisis, if required during an emergency can provide the following:

5.10.1 ICT Support

ICT Support to assist or supplement agencies ICT functions, including:

- Coordination of whole of government ICT resources and activities.
- Whole of government ICT changes (including emergency changes or change freezes).

5.10.2 Cyber security support

Cyber Security support to assist or supplement an agency, including:

- Leading or coordinating investigations activities.
- Threat and risk assessments.
- Intelligence gathering.

5.10.3 Coordination with telecommunications organisations

Work with telecommunications sector organisations to coordinate information sharing, alerting and contribute to situational awareness. This may include arranging briefings, meetings or any other activity deemed necessary in order to assist the response activities. Telecommunications organisations that work with DPC on this activity include, but are not limited to:

- NBN Co
- SingTel Optus Pty Ltd
- Telstra Corporation
- Vocus Group
- Vodafone Hutchison Australia Pty Limited
- TPG Telecom

5.11 Response Levels

The Response Level **(refer Table 3)** will be determined by the needs of the situation and set by the State Controller or Duty Deputy State Controller. The four levels are designed to guide DPC staff on response actions, these may be set when responding in Support or in Control.

The Response Level may also be raised to guide DPC staff on response actions based on an increased level of assessed threat. This may relate to environmental factors, political or economic considerations or national security information.

Table 4 - Response Levels descriptions

Response Levels	General Actions
Business as Usual	Not for Public Version
Elevated	
High	
Severe	

5.12 Rundown

The State Controller or Deputy State Controller will make the determination that a coordinated response can be scaled down and concluded. In the event of a State level declaration, the State Coordinator will make this determination. Activities may include:

- Revoking any temporary arrangements established during the incident
- Notifying all parties involved that the need for a coordinated response has ceased
- Debriefing all members of the IMT
- Collating and recording all written documentation, including copies of personal notes
- Ensuring documents such as the Incident Log are signed off by the Incident Controller
- Ensuring that a formal debrief/post incident review process is performed.
- The Operations Manual contains details of the rundown activities.

5.13 Investigation

Any incident may be subject to a coronial, criminal or other investigation. As directed under the SEMP, the investigating agency will ensure that appropriate investigative procedures are followed. All agencies involved in the Incident, are to ensure that, where possible, physical evidence is not destroyed, and that records and notes are maintained to assist the investigative process.

6 RECOVERY

Recovering from an incident is the coordinated process of supporting those affected by an incident. Recovery processes are likely to commence while response activities are in progress, gaining momentum as the response phase nears completion.

6.1 Transition from Response to Recovery

Recovery requirements will differ depending upon the level and type of the incident. Recovery activities will have commenced at the time that response activities commence. As response activity slows, responsibility for the ongoing management and coordination of the emergency into the recovery phase is transferred from the Control Agency to the state recovery coordinator.

The State Coordinator (SA Police) will appoint an Assistant State Coordinator – Recovery as soon as practicable after a declaration under the Act is made. During an activation of the State Emergency Centre, the State Recovery Office will be represented to help facilitate the assessment of recovery activities.

6.2 State Recovery Committee

The Control Agency for Cyber Crisis has representation on the State Recovery Committee (SRC) as part of the Planning and Preparation arrangements for disaster recovery. Should the State Recovery Committee be convened to assist with an incident for which the Control Agency for Cyber Crisis when is in control, then the Control Agency will be required to be represented on the SRC for the duration of the recovery process.

The State Coordinator will appoint an Assistant State Coordinator – Recovery as soon as practicable after a declaration under the State Emergency Management Act is made. During an activation of the State Emergency Centre, the State Recovery Office will be represented to enable assessment of recovery activities required.

The Control Agency for Cyber Crisis may need to assist the Assistant State Coordinator – Recovery and the State Recovery Office with the assessment of recovery activities required where there is a large Cyber or Telecommunications Crisis.

6.3 Cyber Insurance

SAICORP has a cyber insurance policy that can be accessed by agencies in some cases. The Control Agency for Cyber Crisis will liaise with SAICORP to initiate any cyber insurance claims.

The Control Agency for Cyber Crisis and SAICORP will work with agency finance department as early as possible during the response to an incident to record all associated expenditure so that it can later be assessed by the insurer.

6.4 Financial Impact Assessment

There is a tool designed to assist agencies assess the financial impact of a cyber incident on their agency resources and services. Understanding the resource and financial impacts of an incident can assist with reporting to agency executive management, ministers and boards, and insurance claims.

6.5 Recovery Assessment

There is a form designed to assist agencies, the Control Agency and the State Recovery Office assess disaster recovery requirements following an Incident. The term 'disaster recovery' is used in this context to mean the coordinated process of supporting communities that have been affected by a disaster in the reconstruction and restoration of psycho-social, economic, built and natural environments.

7 Document Approval and Control

Document Control

Assigned Review Period	Review Cycle	Annual
	Next Review Date	01/08/19

Document Review

Title	Name	Date Signed	Signature
Executive Director, ICT and Digital Government	x	x	x
Chief Information Security Officer, ICT and Digital Government	x	x	x
Manager, Cyber Resilience & Emergency Management Coordinator	x	x	x

Document Sign-Off

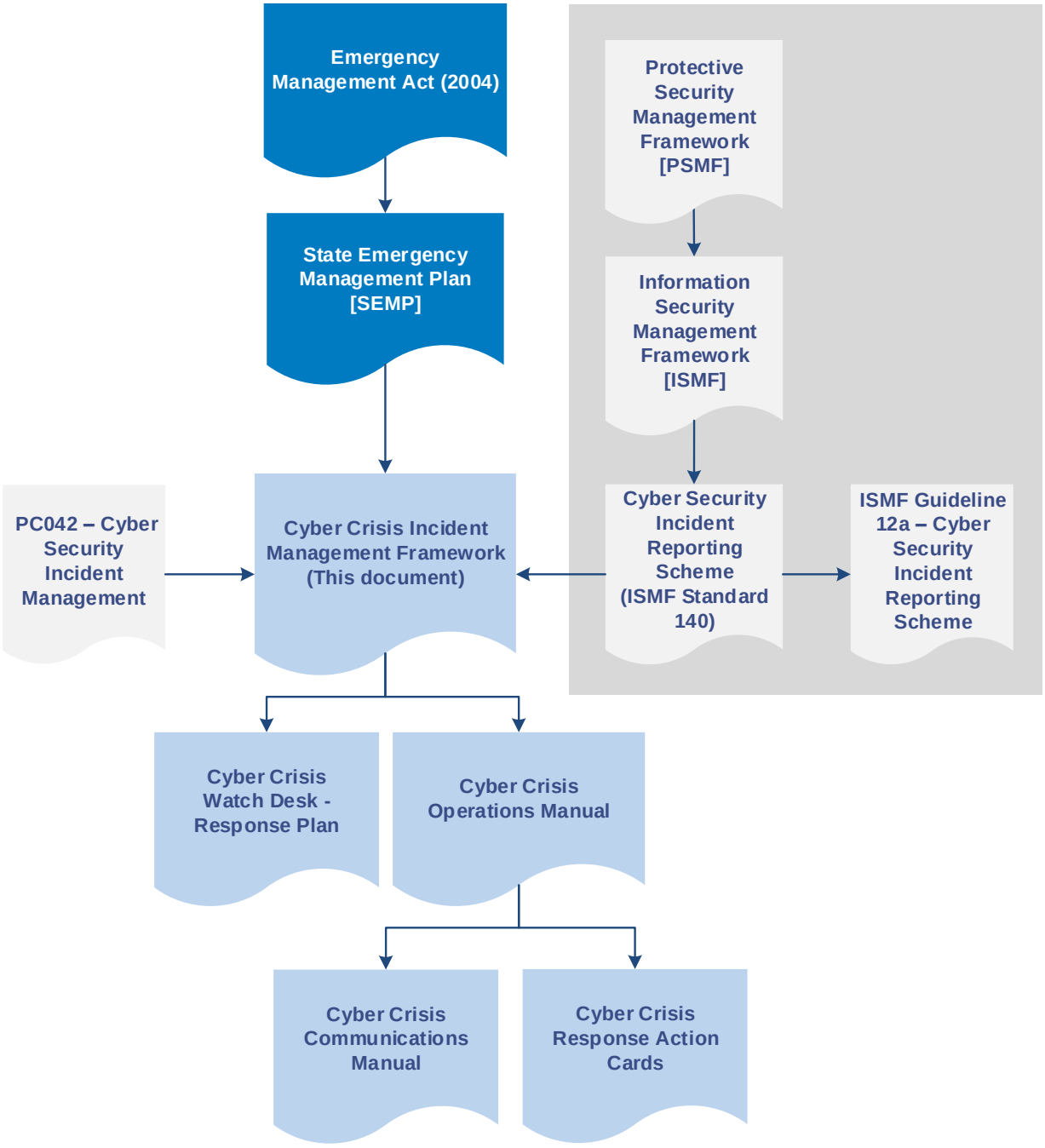
Title	Date Signed	Signature
DPC, Chief Executive	x	x

APPENDIX 1: GLOSSARY

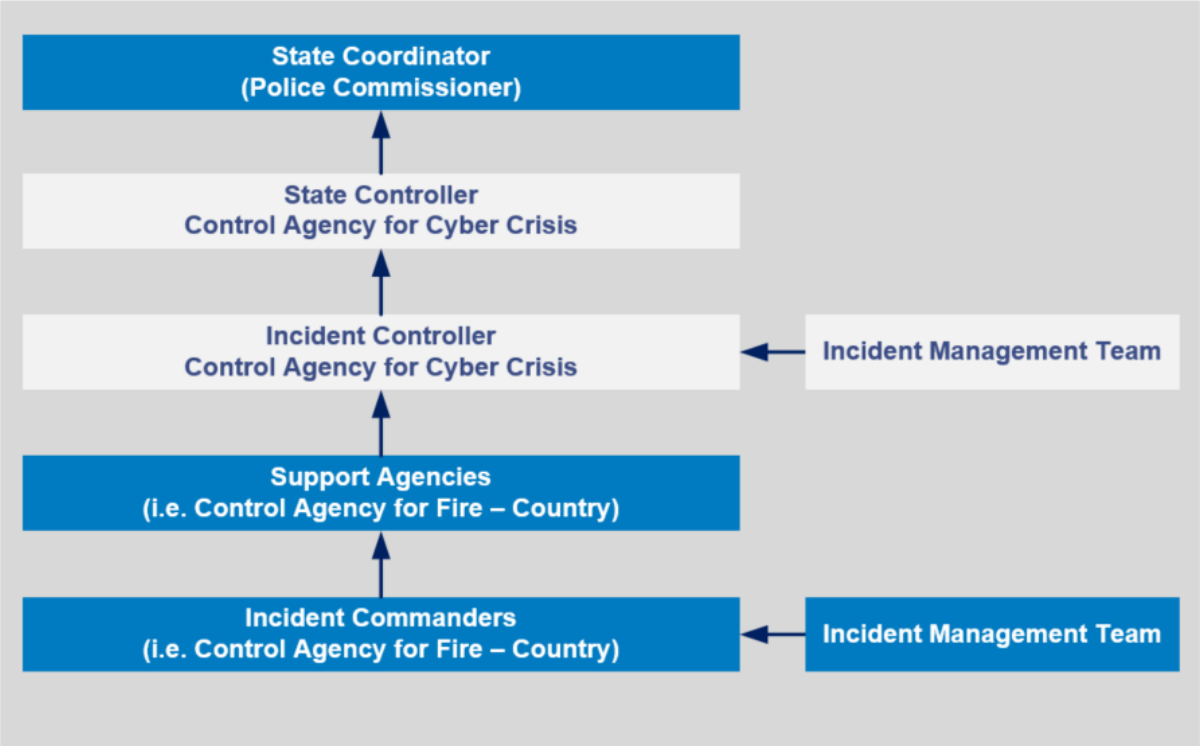
Control	The overall direction of emergency management activities in an emergency situation. Authority for control is established in legislation or in an emergency plan and carries with it the responsibility for tasking other organisations in accordance with the needs of the situation. Control relates to situations and operates horizontally across organisations.
Control Agency	The agency exercising control at an emergency. The agency will be appointed as per Section 20 of the Emergency Management Act 2004.
Command	The internal direction of the members and resources of an agency in the performance of the organisation's roles and tasks. Command operates vertically within an organisation.
Executive Liaison Officer (ELO)	An emergency contact point within each supplier organisation and government agency who will act as the primary contact for the Control Agency in an emergency and will assist the Cyber Crisis Control Agency as required. The Executive Liaison Officer, decision maker at the Executive level as they may be required to act on behalf of their agency during an incident. Typically fulfilled by the Agency Security Executive within a government agency.
Cyber Security	Measures relating to the confidentiality, availability and integrity of information that is processed stored and communicated by electronic or similar means.
DPC	The Department of the Premier and Cabinet. DPC is the Control Agency for Cyber Crisis under the State Emergency Management Plan.
Emergency	An event, actual or imminent, which endangers or threatens to endanger life, property or the environment, and which requires a significant and coordinated response. Any event which arises internally or from external sources which may adversely affect the safety of persons in a building or the community in general and requires immediate response by the occupants. An unplanned situation arising, through accident or error, in which people and/or property are to potential danger from the hazards of dangerous goods. Such emergencies will normally arise from vehicle accident, spillage or leakage of material or from a fire. Note - This is not limited to naturally occurring events (such as earthquakes, floods or storms) but would, for example, include fires, explosions, accidents, epidemics, pandemics, emissions of poisons, radiation or other hazardous agents, hijacks, sieges, riots, acts of terrorism and hostilities directed by an enemy against Australia .
Emergency management	A range of measures to manage risks to communities and the environment. The organisation and management of resources for dealing with all aspects of emergencies. Emergency management involves the plans, structures and arrangements which are established to bring together the normal endeavours of government, voluntary and private agencies in a comprehensive and coordinated way to deal with the whole spectrum of emergency needs including prevention, response and recovery.

Emergency Management Act 2004	The Act that establishes strategies and systems for the management of emergencies in South Australia.
Hazard Leader	The agency because of its legislative responsibility or specialised knowledge, expertise and resources, undertakes a leadership role for planning emergency management activities pertaining to the prevention of, preparedness for, response to, and recovery from a specific hazard. The role is to lead a multi-agency approach to planning for the identified hazard.
Incident Controller	The individual responsible for the management of all incident operations.
ISMF	The South Australian Government Information Security Management Framework. The ISMF is a set of policies, with supporting standards, which address the security of Cyber Crisis assets within the Government of South Australia. The ISMF applies to all South Australian Government agencies and suppliers whose contractual requirements include it.
SEC	State Emergency Centre. The SEC coordinates multi agency responses when there are major emergencies and disasters. This includes declarations under the Emergency Management Act (2004).
SEMP	The State Emergency Management Plan. The Plan outlines responsibilities, authorities and the mechanisms to prevent, or if they occur manage, and recover from, incidents and disasters within South Australia.
State Control Centre	The nominated location from which a functional service coordinates the activities of its participating agencies. This centre may have a dual role if the agency responsible for a functional service is also undertaking response or recovery operations as a control or Support Agency.
Supplier	A company that is a current or potential future provider of services to government. This includes: • Responsible Parties that are suppliers (as defined in the Information Security Management Framework); and • Performing Suppliers which are defined as groups or organisations that are contracted formally or informally to supply goods or services to the State or its agencies.
Support Agency	An agency which provides essential services, personnel, or material to support or assist a Control Agency or affected persons.
the Act	See Emergency Management Act (2004).

Appendix 2 Document hierarchy



Appendix 3 Control Agency Diagram



Appendix 4 Support Agency Diagram