VICTORIAN GOVERNMENT CIO COUNCIL

Information Security

Critical Information Infrastructure Risk Management

Standard

Agencies must identify, assess and mitigate risks to their Critical Information Infrastructure assets.

Keywords:	Critical Information Infrastructure, CII.	
Identifier: SEC STD 02	**Version no.:** 1.0	**Status:** Final
Issue date: 1 October 2012	**Date of effect:** 1 October 2012	**Next review date:** 1 November 2014
Authority: Victorian Government CIO Council	**Issuer:** Victorian Government Chief Technology Advocate	

Requirements

This Critical Information Infrastructure (CII) standard addresses the risks to information and communications technologies (ICT) underpinning critical government services. Agencies must:

- assess their services and ICT assets, identify CII, and record it in a *CII Register* using a provided template;
- assess the health of each CII asset, using a *CII Health Check* template; and
- take appropriate actions to mitigate the risks to the availability, integrity and confidentiality of their CII assets, and report the status of these risk mitigations annually (see *Compliance Reporting* below).

Overview

In recent years, there has been an increasing focus within Australian governments on the protection of Critical Infrastructure and Essential Services, initially in the context of terrorist attacks (particularly in response to the 9/11 attack in the USA in 2001) but more recently in a broader disaster context (e.g. bushfires, floods, etc.)

In Victoria[1]:

- in 2002, the *Final Report: Review of Essential Services* was delivered, and the Victoria became a signatory to the *Intergovernmental Agreement on Australia's National Counter Terrorism Arrangements*;
- in 2003, the *Terrorism (Community Protection) Act* was passed, which provides for government identification of essential services, and government cooperation with the operators of essential services infrastructure for the purposes of risk management; and
- in 2007, the *Victorian Framework for Critical Infrastructure Protection* was introduced.
- in 2009, the Victorian Auditor-General's Office (VAGO) published its report on *Preparedness to Respond to Terrorism Incidents: Essential Services and Critical Infrastructure* , and
- in 2011 the Public Accounts and Estimates Committee published its *Review of the Auditor-General's Report*.

Purpose

This Critical Information Infrastructure (CII) standard addresses the risks to information and communications technologies (ICT) underpinning critical government services.

Critical Infrastructure – terms used

Critical Infrastructure supports the delivery of critical services (defined below.) It is those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or

[1] Silver H., (2011) Presentation to Public Accounts and Estimates Committee: *Managing Risk for Victorian Critical Infrastructure and Essential Services*, Department of Premier and Cabinet, 25 August

rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the State[2].

Critical Information Infrastructure (CII)

The ICT component of Critical Infrastructure is referred to as Critical Information Infrastructure (CII). The subset of CII which is owned, operated, or managed by inner budget (IB) agencies is referred to as IB CII. It **excludes** CII owned or operated by the private sector, or by local, national or other governments.

IB CII is defined as ICT infrastructure upon which **Critical Services** (defined below) are delivered to the community. If this ICT infrastructure is compromised, serious damage could be caused to the State, the government, commercial entities or members of the public[3].

Critical Services

Critical Services are either **Essential** or **Important** government services (defined below), where the loss of confidentiality, integrity or availability of the service would result in serious damage to the physical, social or economic wellbeing of the State[3]. The context for these critical services is:

- the prevention of disasters or crises before they occur, and
- the management of disasters or crises, once they have occurred.

Essential Services

Essential Services are those government services which, if compromised, would endanger or seriously prejudice the life, personal safety, or health of the whole or a section of the community.

Their primary focus is on the protection of the lives of members of the public. Essential Services combat identified threats, protect the physical survival of the people in a community, and maintain the continuity of executive government (which needs to make decisions to protect the safety of citizens during a crisis or disaster)[3].

Essential Services can usually be identified by asking the question: If the availability, confidentiality or integrity of this service was compromised:

- could the life of any person be put in danger; or
- would any Executive Government decision making, which could prevent a disaster or crisis (and loss of life), or could save lives during a disaster or crisis, be adversely impacted?

To be categorised as an essential service, the adverse impact of a compromised service must be direct, not indirect. As an example from the health sector, inadequate funding of the health budget could ultimately lead to loss of life, but this is too indirect. However, the non-availability of hospital emergency services could directly lead to loss of life, so this is an essential service.

The criticality of some essential services depends on time e.g. when considering the availability of some essential services, loss of life might be unlikely to occur if a service is unavailable for a few hours, but likely if

[2] Adapted from Australian Government, *Critical Infrastructure Resilience Strategy*

[3] Adapted from Government of South Australia, OCIO/G4.3, ISMF Guideline 3, *Critical Information and Communication Technology*.

the service is not available for greater than six months. As an example, this could be the case for prescribed burning to reduce the likelihood of future bushfires, which is still an essential service, despite the long term impact.

Saving lives (Essential Services) is the first priority in a crisis or disaster. Saving property and protecting other assets which contribute to the **quality of lives** of members of the public is the second priority (see Important Services below).

Important Services

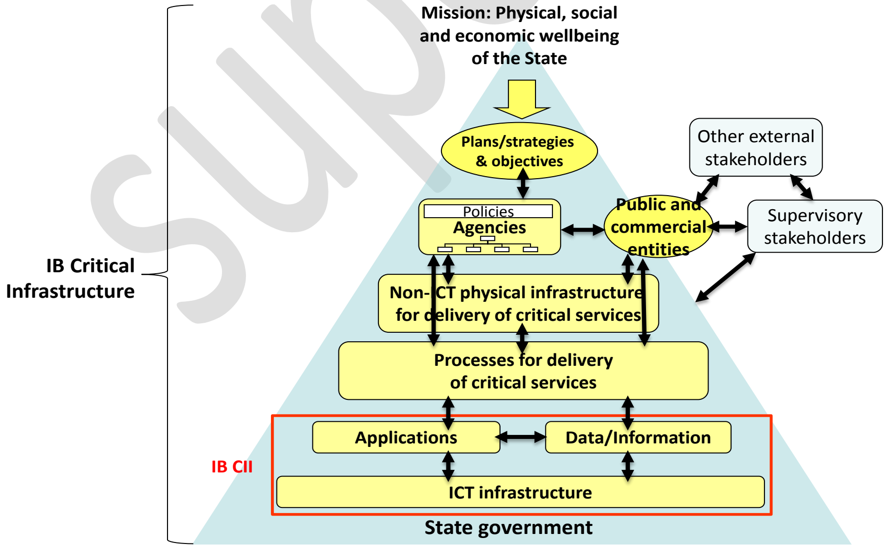
Important Services are those services that are directly related to the physical, economic, legal and psycho-social safety and security of the community, business and government[4]. Important Services go beyond protecting people to protecting the property, organisations and environments where people live and work i.e. they protect the quality of life of citizens. The context for these important services is the same as the context for essential services i.e. the service must be related to:

- the prevention of other disasters or crises (which do not involve loss of life), before they occur; or
- the management of responses to these other disasters or crises, once they have occurred.

Summary of context

To summarise the context for the terms used in this policy, Figure 1 shows that essential and important services are delivered by IB agencies, who invest in, or fund, the physical infrastructure associated with the delivery of these services. They also organise themselves to deliver these services by implementing and managing appropriate processes. These processes are supported by IB CII i.e. by IB-agency-managed software applications which create and use data and information. The applications and data typically run on IB-agency-managed (or contracted third party managed) ICT infrastructure, including servers, networks, computer rooms, etc.

Figure 1: Context for IB CII


Mission: Physical, social and economic wellbeing of the State
Plans/strategies & objectives
Other external stakeholders
Policies
Agencies
Public and commercial entities
Supervisory stakeholders
IB Critical Infrastructure
Non-ICT physical infrastructure for delivery of critical services
Processes for delivery of critical services
Applications
Data/Information
IB CII
ICT infrastructure
State government

Rationale

IB CII underpins government services that protect the lives and property of members of the public, and supports their social and economic well-being. Any compromise of IB CII can have a direct adverse impact on citizens, and lower their trust and confidence in government information systems and services.

Derivation

- SEC POL 01 Information Security Management Policy; and
- SEC STD 01 Information Security Management Framework

Scope

This standard applies all departments; Victoria Police, VicRoads, State Revenue Office, and the Environment Protection Authority; and any shared services providers (third parties)[4] including CenITex. These organisations are collectively referred to as department and agencies (D&A) in this standard.

Where applicable, legal and or regulatory compliance obligations take precedence over this policy and standards. Departments and agencies may have additional legal and or regulatory information protection compliance requirements. Examples include (but are not limited to) Victoria Police and the Commissioner for Law Enforcement Data Security (CLEDS), credit card processing contract obligations of the Payment Card Industry Data Security Standard (PCI DSS) and the Information Privacy Act 2000.

Compliance

Timing

From the date of effect on the front of the document.

Reporting

Mandatory annual *CII Health Check* (SEC TEMP 2-2) reports will be in accordance with the framework and report template developed in conjunction with the Victorian Managed Insurance Authority (VMIA), and must be completed by the end of December each calendar year.

The *CII Health Check* (SEC TEMP 2-2) must be submitted to the agency Risk and/or Audit committee, and the agency Executive. A copy of the report and related minutes of the Risk and/or Audit committee must be provided.

The annual *CII Health Check* (SEC TEMP 2-2) will ensure executive visibility and oversight of the information security risks to critical services and supporting ICT assets.

[4] Some examples of shared service provider within Victorian Government are CenITex, eduPay and Shared Business Systems (SBS). D&A's may have third parties providing similar services.

Agency *CII Health Check* (SEC TEMP 2-2) reports will be consolidated into a Victorian Government summary for review by the State Coordination and Management Council (SC&MC), the DSLG, and the CIO Council.

The compliance schedule for CII asset SRMPs, SSPs and SOPs

Systems Risk Management Plans (SRMPs), Systems Security Plans (SSPs) and Standard Operating Procedures (SOPs), are requirements mandated by the Australian Government Information Security Manual (ISM). They must be developed for all CII assets by 30 June 2013.

The implementation of these SRMPs, SSPs and SOPs may carry forward beyond 30 June 2013. Agencies should list the most important Urgent, Tactical, and Strategic risk mitigations that need to be implemented, submit them to their CISO for approval, and report progress against these risk mitigations in annual CII reporting.

Reference and Toolkits

Victorian Framework for Critical Infrastructure Protection:
http://www.g21.com.au/dmdocuments/HWB-R-0704-167.pdf

Victorian CII Register and CII Health Check templates:
http://digital.vic.gov.au/policies-standards-guidelines/information-security/

Australian Government Information Security Manual: http://www.dsd.gov.au/infosec/ism/index.htm

Information on the development of security risk management plans can be found in the Information Security Risk Management Guidelines available from Standards Australia at: http://www.standards.org.au

Information relating to the Information Security Management Framework is contained in the Australian Government Information Security Management Protocol of the Protective Security Policy Framework.

Australian Government PSPF Policy: http://www.protectivesecurity.gov.au/Pages/default.aspx

Australian Government PSPF Glossary of Terms:
http://www.protectivesecurity.gov.au/pspf/Pages/PSPF-Glossary-of-terms.aspx

Australian Government National Information Infrastructure (NII):
http://www.afp.gov.au/media-centre/publications/platypus/previous-editions/2001/march-2001/protect.aspx

Further information

For further information regarding this standard, please contact digital.government@dsdbi.vic.gov.au.

Glossary

Term	Meaning
CII	Critical Information Infrastructure (See *Terms Used*)
Critical Services	See *Terms Used*
Essential Services	See *Terms Used*
IB	Inner budget (11 Departments and VicRoads, VicPolice, Environmental Protection Authority (EPA) and State Revenue Office (SRO) and CenITex)
Important Services	See *Terms Used – Victorian Framework for Critical Infrastructure Protection*
VG	Victorian Government

Version history

Version	Date	TRIM ref	Details
0.1	15 June 2012	N/A	Initial Draft
1.0	26 July 2012	D12/157453	Final revisions for Board approval
1.0	31 August 2012	D12/157453	Final text revisions for release to CIO Council