Office of the Victorian Information Commissioner

INFORMATION FOR AGENCIES

Victorian Protective Data Security Standards (VPDSS) and the Critical Infrastructure Risk Management Program (CIRMP)

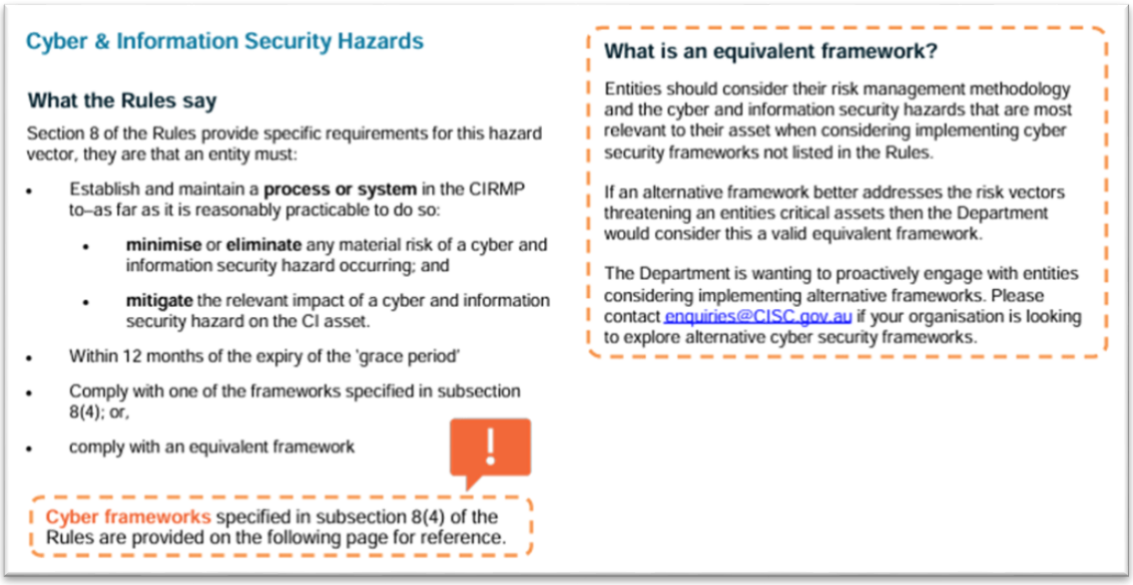
Using the VPDSS as an equivalent framework for CIRMP obligations

The Department of Home Affairs - Cyber and Security Infrastructure Centre (**CISC**) has published *Guidance for the Critical Infrastructure Risk Management Program*[1]. A CIRMP is a written program that identifies and manages 'material risks' of 'hazards' that could have a 'relevant impact' on a Critical Infrastructure (**CI**) asset. Part 2A[2] of the Security of Critical Infrastructure Act 2018 (**SOCI Act**) sets out the requirement to adopt and maintain a CIRMP.

See below for an extract of the cyber and information security hazards as explained under *Section 3: CIRMP rules in practice*:

[1] https://www.cisc.gov.au/resources-subsite/Documents/guidance-for-the-critical-infrastructure-risk-management-program.pdf

[2] https://www.cisc.gov.au/resources-subsite/Documents/cisc-factsheet-risk-management-program.pdf



Cyber & Information Security Hazards

What the Rules say

Section 8 of the Rules provide specific requirements for this hazard vector, they are that an entity must:

- Establish and maintain a **process or system** in the CIRMP to–as far as it is reasonably practicable to do so:
  - **minimise** or **eliminate** any material risk of a cyber and information security hazard occurring; and
  - **mitigate** the relevant impact of a cyber and information security hazard on the CI asset.
- Within 12 months of the expiry of the 'grace period'
- Comply with one of the frameworks specified in subsection 8(4); or,
- comply with an equivalent framework

Cyber frameworks specified in subsection 8(4) of the Rules are provided on the following page for reference.

What is an equivalent framework?

Entities should consider their risk management methodology and the cyber and information security hazards that are most relevant to their asset when considering implementing cyber security frameworks not listed in the Rules.

If an alternative framework better addresses the risk vectors threatening an entities critical assets then the Department would consider this a valid equivalent framework.

The Department is wanting to proactively engage with entities considering implementing alternative frameworks. Please contact enquiries@CISC.gov.au if your organisation is looking to explore alternative cyber security frameworks.

To support Victorian Public Sector (**VPS**) organisations complying with the CIRMP rules, OVIC met with the CISC team to discuss synergies between some CIRMP requirements and the Victorian Protective Data Security Framework and Standards (**VPDSF/S**).

OVIC proposes that by using the VPDSS, including undertaking a Security Risk Profile Assessment (**SRPA**) and developing, implementing, and maintaining a Protective Data Security Plan (**PDSP**), VPS organisations align with the CIRMP rules for identifying, assessing, and managing the cyber and information security risks to CI assets.

For VPS organisations to comply with the CIRMP rules, they will need to document the following in their submission form to the CISC. Organisations can use the suggested wording below to assist in their submission:

Why has the entity selected a specific cyber security framework not listed in the rules?	As a Victorian Public Sector (VPS) organisation, we are legislated to comply with section 88 *Compliance with the protective data security standards* of the Privacy and Data Protection Act (2014). As such we are already following an equivalent framework that can be used for the purposes of demonstrating compliance with the CIRMP rules.
How did the entity assess this framework to be an equivalent framework?	The Victorian Protective Data Security Standards (VPDSS or Standards) establish 12 mandatory requirements to protect public sector information and systems across all security areas including governance, information,

	personnel, Information Communications Technology (ICT) and physical security. The VPDSS provide a set of criteria for the consistent application of risk-based practices to minimise information security risks and incidents similar to the principles of the CIRMP rules. The standards are supported by *VPDSS Implementation Guidance* containing elements (controls that directly modify risk and supportive controls) for general VPS environments. In addition to this, we apply the *VPDSS Implementation Guidance for Industrial Automation and Control Systems (IACS)*. This targeted guidance contains additional elements specific to IACS environments. The VPDSS is developed to help Victorian public sector organisations: • manage public sector information and systems throughout its lifecycle (creation to disposal); • manage public sector information and systems across all the security areas (governance, information, personnel, Information Communications Technology (ICT), physical); • manage security risks to the confidentiality, integrity, and availability (often referred to as CIA) of public sector information and systems; • manage external parties with access to public sector information and systems; • share public sector information with other organisations with confidence; and • minimise security incidents.
How does the entity use that equivalent framework in their RMP?	We undertake a Security Risk Profile Assessment (SRPA) and develop, implement, and maintain a Protective Data Security Plan (PDSP), as required by the Privacy and Data Protection Act (2014). This includes identifying, assessing, and managing the cyber and information security risks to CI assets.

	The SRPA and PDSP are regularly reviewed in line with normal risk management processes to: • continue to manage information and systems' risks; • ensure agency head visibility; and • report on progress to OVIC as required by the Privacy and Data Protection Act (2014).

By adhering to the VPDSS, VPS organisations operating CI assets will be seen to satisfy the last bullet point "comply with an equivalent framework" of CIRMP Section 8 of the Rules.

More information

For further information on the *VPDSS Implementation Guidance* and *VPDSS Implementation Guidance for Industrial Automation and Control Systems* visit our website: https://ovic.vic.gov.au/information-security/information-security-resources/implementation-guidance-for-industrial-automation-and-control-systems/

We welcome your feedback on this document. Contact OVIC at security@ovic.vic.gov.au to discuss this further.

Disclaimer

The information in this document is general in nature and does not constitute legal advice.

Organisations must perform their own due diligence to satisfy themselves that they are complying with their information security obligations and to ensure that any information they provide to CISC is true and correct.