

# Security Risk Management Plan

## What is a Security Risk Management Plan?

A strategic Security Risk Management Plan (SRMP) is a foundation document which communicates the issues that are important to an organisation from a security risk management perspective and to address the issues. A SRMP links the security program to wider corporate or government strategies.<sup>1</sup>These linkages become crucial in justifying budget allocations and form the basis for operation security planning and decision making.

Security risk management planning assists decision-making by:

- Applying appropriate controls effectively and consistently
- Adapting to change while safeguarding the delivery of business and services
- Improving resilience to threats, vulnerabilities and challenges
- Driving protective security performance improvements

---

*A security risk management plan does not have to be complex, but it does have to be contextually relevant.*

---

The purpose of the SRMP is a best practice approach to identifying and reducing potential security risks. Depending on the documentation framework chosen, multiple systems could refer to, or build upon, a single SRMP.

This document's purpose is to provide a basic security framework for the systems in scope for review.

- Controls listed within the SoA will be used to determine that the SRMP is comprehensive and appropriate for the environment
- The SRMP needs to identify assessed risks to key assets and information and detail the risk treatments implemented

This document is created when assessing the security aspects of the systems in scope for review. The SRMP is created to define the mitigation strategy of the identified security risks documented through the Statement of Applicability (SoA), and through analysis of systems in scope for review.

---

<sup>1</sup> Draper, R. 2014. <https://www.linkedin.com/pulse/how-write-strategic-security-rick-draper>



A security risk management plan typically includes:

1. Goals and objectives towards effective SRM and expectations to provide a positive security culture;
2. Security risk environment, including:
  - a. What the organisation needs to protect: people, information and assets assessed as critical to its ongoing operations;
  - b. What the organisation needs to protect against;
  - c. How the risk will be managed within the organisation;
3. Risk tolerance;
4. Security capability, which refers to the maturity of an organisation's capability to manage security risks; and
5. Security risk management strategies, including: Identifying how it will apply controls to respond to internal or external threats.<sup>2</sup>

### Why is a Security Risk Management Plan important?

A SRMP identifies information security risks and defines appropriate mitigation measures for systems. An SRMP consists of threat risk assessment and applicable risk treatment strategies. Within the Australian Government Information Security Manual, an SRMP is considered a core security document and key component of an agency's information security framework.<sup>3</sup>

---

*Risk analysis helps establish a good security posture, risk management keeps it that way.*

---

A SRMP ensures that threats to your organisations are handled in an integrated and cost-effective manner. SRMPs also ensure that the security incidents towards other players by do not impact your organisation's activities. Risk reducing measures ensure you are able to stay competitive if you experience a crisis.<sup>4</sup>

Three key benefits to having a SRMP are:

1. An SRMP maximises potential for forecasting and competitiveness
2. Employees feel secure in forward-looking goals and are able to fulfil objectives
3. An SRMP ensures organisational controls over intellectual property

---

<sup>2</sup> Australian Government: Attorney-General's Department. 2018.

<https://www.protectivesecurity.gov.au/governance/security-planning-risk-management/Pages/default.aspx>

<sup>3</sup> Foresight, 2018. <https://foresight.net.au/threat-and-risk-assessments/>

<sup>4</sup> Safetec, 2018. <https://www.safetec.no/en/services/risk-management/security-risk-management/>





## About Cogito Group

Cogito Group is an award winning Australian owned and operated ICT company specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.



**AUSTRALIAN  
TECHNOLOGIES  
COMPETITION**  
**CYBER  
SECURITY  
AWARD**

**2018**  
**Land Forces**  
AUSTRALIA INDO ASIA PACIFIC  
INNOVATION AWARD FINALISTS




**>55th Australian  
Export Awards**  
**2017 NATIONAL FINALIST**



 **Cogito Group**

 [www.cogitogroup.net](http://www.cogitogroup.net)

 Canberra: +61 2 6140 4494  
Wellington: + 64 4909 7580