Fact Sheet

Cogito Group

Security Risk Management Plan

What is a Security Risk Management Plan?

A strategic Security Risk Management Plan (SRMP) is a foundation document which communicates and addresses issues important to an organisation from a security risk management perspective. A SRMP links security programs to wider corporate or government strategies.[1] 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 through:

- 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.

The Purpose of a SRMP

The purpose of SRMPs 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.

The document's purpose is to provide a basic security framework for the systems in scope for review. Controls listed within the Statement of Applicability (SoA) are used to determine whether the SRMP is comprehensive and appropriate for the environment. The SRMP additionally must identify assessed risks to key assets and information and detail the risk treatments implemented.

SRMPs are created when assessing the security aspects of the systems in scope for review. They define the mitigation strategy of the identified security risks documented in the SoA, and through analysis of systems in scope for review.

Security Risk Management Plan

Fact Sheet

Components of a SRMP

A SRMP typically includes:

- Goals and objectives towards effective Security Risk Management and expectations to provide a positive security culture.
- An overview of the Security Risk Environment, including:
  - What the organisation must protect, such as people, information, and assets assessed as critical to its ongoing operations.
  - Potential threats the organisation must defend itself from.
  - How the risk will be managed within the organisation.
- Risk tolerance.
- Security capability, such as the maturity of an organisation's capability to manage security risks.
- Security risk management strategies and identifying how the organisation will apply controls to respond to internal or external threats.[2]

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

Benefits of a SRMP

Three key benefits of SRMPs are:

- SRMPs maximise potential for an organisation's forecasting and competitiveness.
- Employees feel secure in forward-looking goals and can fulfil objectives.
- SRMPs ensure organisational controls over intellectual property.
- Risk analysis helps in establishing good security posture and risk management helps in maintaining such posture.

Why is a Security Risk Management Plan Important?

A SRMP identifies information security risks and defines appropriate mitigation measures for systems. A SRMP consists of threat risk assessments and applicable risk treatment strategies. Within the Australian Government Information Security Manual, SRMPs are considered a core security document and key component of an agency's information security framework.[3]

A SRMP ensures that threats to your organisations are handled in an integrated and cost-effective manner. Risk reducing measures ensure an organisation can remain competitive whilst experiencing a crisis.[4]

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.

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

[2] Australian Government: Attorney-General's Department. 2018. https://www.protectivesecurity.gov.au/governance/security-planning-risk-management/Pages/default.aspx

[3] Foresight, 2018. https://foresight.net.au/threat-and-risk-assessments/

[4] Safetec, 2018. https://www.safetec.no/en/services/risk-management/security-risk-management/