Fact Sheet

Cogito Group

System Security Plan

What is a System Security Plan?

The purpose of a System Security Plan (SSP) is to provide an overview of the security requirements of a system and describe the planned or implemented controls to meet those requirements. SSPs outline responsibilities and expected behaviour of all individuals who access the system, and provides a structured process for planning adequate, cost-effective security protection for a system. SSPs reflect input from individuals with varying responsibilities concerning the system, including functional end-users, information-owners, the system administrator, and the system security manager. [1]

SSPs are proposed as plans to protect and control an information system or plan that is already in implementation. They are created using the organisation/IT environment security policy as the benchmark.

Components of SSPs

SSPs typically include:

- A list of authorised personnel/users that can access the system.
- Levels of accessed/tiered access, or what each user is allowed and not allowed to do on the system.
- Access control methods, or how users will access the system (user ID/password, digital card, biometrics).
- Strengths and weaknesses of the system and how weaknesses are handled.
- System backup and restoration procedures.
- Plan development for security in the lifecycle of the system.
- System boundary analysis and security controls.
- Basic contents, including system description, description of controls, system security roles and responsibilities, external requirements, information categories, interconnectivity with the system, certification level, and plan information.

SSPs are created when assessing the security aspects of the systems in scope for review, defining the mitigation strategy of the identified security risks documented in the Security Risk Management Plan (SRMP) and Statement of Applicability (SoA).

SSPs must:

- Address the specific circumstances of the organisation and must be based on an industry–recognised approach to risk management and methodology.
- Be suitably assessed by the organisation to confirm the products are fit for purpose.
- Describe the security controls for the systems in scope for review.
- Determine that the SSP is comprehensive and appropriate for the environment based upon controls listed within the SoA.
- Describe any risk controls implemented.
- Outline the responsibilities and expected behaviour of all individuals who access the system.

Why are SSPs Important?

A well-documented SSP should act as a single reference for what needs to be secured, control documents, support oversite, forecasting, planning and budgeting, and align with document compliance. SSPs should clearly identify which security controls used scoping guidance and include a description of the type of considerations that were made. The key benefits of SSPs are the assessment of risk, detailing organisation-specific security requirements, providing cost-benefit analyses, and detailing the availability of compensating controls.

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]SANS Asia Pacific, System Security Plan Development Assistance Guide 2003, SANS, https://www.sans.org/projects/systemsecurity.php