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 the system and describe the controls in place or planned to meet those requirements. The SSP outlines responsibilities and expected behaviour of all individuals who access the system. The SSP provides a structured process for planning adequate, cost-effective security protection for a system. SSPs reflect input from various individuals with responsibilities concerning the system, including functional end users, information owners, the system administration ad the system security manager.[1]

SSP is not: proof of the existence of controls, a security procedures manual, and should not be lengthy and unusable

---

SSP is proposed as a plan to protect and control an information system, or a plan that is already in implementation. I to usually created using the organisation/IT environment security policy as the benchmark.

The SSP typically includes:

- A list of authorised personnel/users that can access the system;
- Level 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; and
- Basic contents, including: system description, description of controls, system security roles and responsibilities, external requirements, information categories, interconnectivity with the system, certification level, plan information.

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

This SSP is created when assessing the security aspects of the systems in scope for review.

The SSP is created to define the mitigation strategy of the identified security risks of documented through the Security Risks Management Plan (SRMP) and Statement of Applicability (SoA), and through analysis of systems in scope for review.

The document needs to address:

- Security documentation should relate to the specific circumstances of the organisation and be based on an industry–recognised approach to risk management and methodology, as described in the SSP (template) appendices.
- This document needs to be suitably assessed by the organisation to confirm the products are fit for purpose.
- his document's purpose is to describe the security controls for the systems in scope for review.
- Controls listed within the SoA will be used to determine that the SSP is comprehensive and appropriate for the environment
- The SSP needs to describe the risk controls implemented

Why is a System Security Plan 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
- Align with document compliance[2]

SSP should clearly identify which security controls used scoping guidance and include a description of the type of considerations that were made. The key functions of an SSP are:

- Assessment of risk
- Organisation-specific security requirements
- Specific treat information
- Cost-benefit analyses
- Availability of compensating controls
- Special circumstances

[2] Hester, Donald E. 2014, Maze and Associates, https://www.slideshare.net/sobca/system-security-plans-101.

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.

Cogito Group
www.cogitogroup.net
Canberra: +61 2 6140 4494
Wellington: + 64 4909 7580