Cogito Group

Statement of Applicability

What is a Statement of Applicability?

A Statement of Applicability (SoA) is the central document that defines how you will implement a large part of your information security. The SoA is the main link between the risk assessment and treatment and the implementation of your information security – its purpose is to define which of the controls from the Australian Government Information Security Manual (ISM) will be applied and implemented.

This document is created when assessing the security aspects of a system(s) in scope for review. The SoA is used to define the security baseline.

Any identified items from the SoA are linked to the SRMP document which is created to document the security threats and risks related to the systems in scope for review.

The SoA is created along with the SRMP and as a precursor to the SSP.

This document needs to be suitably assessed by the organisation to confirm the products are fit for purpose.

- This document's purpose is to provide a basic security framework for the systems in scope by identifying which of the Information Security Manual (ISM) controls are applicable, compliant or non-compliant
- Controls listed within the SoA will be used to determine that the SRMP is comprehensive and appropriate for the environment

Why is a Statement of Applicability important?

Full attention and focus on the SoA during its preparation should result in few or no surprises. If the SoA is created correctly, nothing major can fall through the cracks regarding conformance to information security requirements. Any nonconformance/noncompliance found by the auditors could be considered as extra resources that would help organizations toward continual improvements.[1]

[1] ISACA, 2017. Benefits of the Statement of Applicability in ISMS.

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