About ISM3

Today's ISMS Challenge

Information Security Management Systems (ISMS) aim to provide a comprehensive approach towards effective management of information security. Approaching information security from a technical perspective does provide security for specific areas of an organization; e.g., wireless network, perimeter, desktops, etc.

The big question that the ISMS community needs answering is "How do you integrate these stand-alone security solutions under one common framework and integrate it with the business goals of the organization?"

The answer to date has centered largely on the ISO/IEC 27000 series. Increasingly however, business managers are demanding more measurement-based information on how effectively their ISMS is performing, so they can optimize their return on investment security community has answered this question by developing frameworks (standards), which can be used to develop a comprehensive information security management framework. Significant amongst them have been ISO/IEC 27001.

ISM3 Objectives

1. Fill the gap between the ISMS capability as defined in ISO27001, the catalog of best practice controls identified in ISO27002, and the need that information security management personnel have to continually improve their internal security management using metrics and maturity models.

2. Enable organizations to identify and achieve levels of information security management appropriate to their industry, risk profile, and size.

3. Provide organizations with certification opportunities, such that organizations that have certified their information security management program at a given level of ISM3 can be recognized for their program maturity, and can thus provide some independent level of assurance to their customers as to the rigor with which they treat information security.

4. Provide the basis for an industry ecosystem to develop around the information security management area (much like an enterprise architecture ecosystem has built up around TOGAF), including for trainers on ISM3 methodology, certification of ISM3 implementations and practitioners, and possibly for software providers of information security management tools.

The O-ISM3 standard

The Open Group Information Security Management Maturity Model (O-ISM3) standard defines a framework for

- managing information security in terms of a library of security processes that can be configured to implement specific security controls that match an organization's stated business goals
- monitoring the outcomes of those processes in terms of measurements which indicate their effectiveness.

Each process defines “what” is to be managed, “why” it adds value when managed, “how” it will be managed in terms of the security controls that will be used, and which operational metrics and their allowable variances will be monitored to check the outcomes of those controls.

Security can then be improved by using those measurements to inform business management decisions on which areas in their Information Security Management System (ISMS) they should address so as to yield best return on investment to achieve their required risk profile.

Compatibility with ISO/IEC27001

Open Group Guide: Optimizing ISO/IEC 27001 using O-ISM3, July 2012, G125, published at https://www2.opengroup.org/ogsys/catalog/G125

ISO/IEC 27001 and O-ISM3 are fully compatible. It is straightforward to implement an ISMS that supports both ISO/IEC 27001 and O-ISM3. There are no incompatible issues between these standards:

An organization using ISO/IEC 27001 as its ISMS can map existing controls and documents with corresponding O-ISM3 processes, documents, and outputs, and then measure and analyze the metrics that become available, so producing performance information which will inform security managers on how to most cost-effectively improve their ISMS, on a continuous cycle of operations.

The design of an O-ISM3 implementation can take ISO/IEC 27001 as all or part of its compliance requirement, and map its processes and documents with corresponding ISO/IEC 27001 controls and documents, creating an ISMS that is supportive of both standards.

Using ISM3 with TOGAF and SABSA

Combining The Open Group Standards, O-ISM3 and TOGAF®, with the SABSA® Framework, July 2013, W133, published at https://www2.opengroup.org/ogsys/catalog/W133

The Open Group Information Security Management Maturity Model (O-ISM3) defines a range of security control processes for selective deployment in an enterprise’s Information Security Management System (ISMS) to meet specific ISMS business targets. Each process provides metrics feedback on how effectively it plays its part in meeting the ISMS targets.

This White Paper explains to Enterprise and Security Architects using the TOGAF standard and SABSA framework how the O-ISM3 standard is a valuable resource for aligning security management to the business goals of their ISMS, and also to Operational Security Managers on understanding how the linkage between upstream architecture/design work and downstream operations can be used to influence architects and designers to provide the most optimal security management capabilities and solutions.

Using ISM3 with the CPNI 20 Critical Security Controls (CSC)

Using the O-ISM3 Standard with the CPNI 20 Critical Security Controls (CSC) for Effective Cyber Defense, Dec 2013, W137, published at https://www2.opengroup.org/ogsys/catalog/W137

This White Paper explains how enterprises using the 20 Critical Security Controls (CSC) framework for Effective Cyber Defense can benefit significantly from using The Open Group's O-ISM3 standard to develop and align their ISMS implementation to incorporate those 20 cybersecurity defense measures. The primary audiences for this white paper are ISMS practitioners who have adopted the O-ISM3 Standard to use this paper as expert guidance on mapping O-ISM3 processes to implement the 20 CSC, and to show ISMS practitioners who want to implement the 20 CSC how using the O-ISM3 Standard will enable them to achieve this in their ISMS as a comprehensive, cost-effective and adaptive solution.