ITAM and Information Security

Using 27001:2013 and 19770-1:2017 Together

19770

Contents

- Interdependence of ISM and ITAM
- Common design approaches
  - Risk management
  - Selection of objectives from a normative annex
  - Documentation needed for assessment
- Other linkages from 19770-1
- Driving effective integration
- Other ITAM/ISM standards
- Other observations
- Take-up opportunities
- Resources

Interdependence of ISM and ITAM

- General principle: You can't manage what you don't know. Both ISM and ITAM require complete and accurate knowledge of assets
- The top two critical security controls are ITAM controls (see resources at end)
  - #1: Inventory of Authorized and Unauthorized Devices
  - #2: Inventory of Authorized and Unauthorized Software
- Asset management is the first requirement of the framework core of the US Cybersecurity Framework (NIST, 12 Feb 2014)

Common Design Approaches

- Risk management
- Selection of objectives from a normative annex
- Documentation needed for assessment

Risk Management

- Risk assessment
  - 27001, 6.1.2 Information security risk assessment
  - 19770-1, 6.1.2 IT asset risk assessment
- Risk treatment
  - 27001, 6.1.3 Information security risk treatment
  - 19770-1, 6.1.3 IT asset risk treatment

Selection from Annex

- 27001: Select control objectives (and related controls) from normative Annex A. Selection is by elimination – all not included must be justified.
- 19770-1: Select process objectives from normative Annex A. Selection is by addition – justification must be given for those chosen
  - ‘Tiers’ are pre-defined groupings of process objectives, as defined in Annex B.
    - Tier 1: Trustworthy data: already included in base text
    - Tier 2: Lifecycle integration: all lifecycle processes
    - Tier 3: Optimization: remaining functional processes e.g. contract management

Assessment Documentation

- Statement of Scope
- Statement of Applicability

6.2.2 IT asset management objectives for operation processes

The organization shall determine the objectives which are appropriate for the operation processes identified in 6.2.1. The objectives determined in this way shall be compared with those in Annex A.

A Statement of Applicability shall be produced which lists the objectives specified, with justification for inclusion and exclusion of any listed in Annex A.

NOTE 1 The processes and process objectives listed in Annex A are not exhaustive and additional operation processes and process objectives can be needed.

NOTE 2 The term 'Statement of Applicability' has been chosen because of its analogy with the Statement of Applicability in ISO/IEC 27001:2013. The Statement of Applicability together with the scope definition (4.3) are needed by any internal or external party to understand what is covered by the IT asset management system.

NOTE 3 It is possible but not required to specify groupings of processes and process objectives for inclusion or exclusion based on their tier classification as described in Annex B.

Other Linkages from 19770-1

- Added to Clause 4.2, a note that stakeholders (27001 and 20000-1 use the term ‘interested parties’ – both are acceptable for ISO) include those responsible for related systems and processes, such as for Information Security Management, and Service Management
- Added to Clause 5.2, requirements that the IT asset management policy shall be consistent with (a) the strategic plans of any other management systems used by the organization; and with (b) the relevant policies of any other management systems used by the organization.

Driving Effective Integration

- Integrated management systems for ISM and ITAM
- Common membership of key committees (e.g. change management board)
- Common high-level corporate/organizational policies
- Common reporting lines
- Improved tools

Tools

- Trending towards functional convergence, but not there
- Timeliness
  - ISM: Requires immediate availability of information
  - ITAM: Often just used for periodic license compliance
- Coverage
  - ISM: Identification most important; knowledge of all instances generally not
  - ITAM: Generally requires knowledge of all instances
- Authorization focus
  - ISM: Critical
  - ITAM: Typically weak functionality

Other ITAM/ISM Standards

- 19770-2:2015 Software Identification Tag
  - Facilitates security automation
  - Mandatory per US Department of Defense IT Standards Registry
  - Supported by publications from NIST, Trusted Computing Group, etc
  - See also tagvault.org

Other Observations

- Inventory of Information: in 27001, not in 19770-1

Take-Up Opportunities

- Any organization looking to implement 27001 or 19770-1
- Consultancy organizations helping to implement either
- Certification bodies wishing to extend certifications

- Promotional/engagement
  - Joining WG21 or the 19770-1 development group
  - Blogging, posting etc
  - Presenting at conferences

Resources

- Critical Security Controls a.k.a. Center for Internet Security Controls (CIS Controls)
  - sans.org/critical-security-controls
  - cisecurity.org/controls
- m-assure.com website
  - This presentation and video
  - More information about the ISO ITAM standard
  - More information about the ITIL SAM/ITAM Guide
  - Contact information