Generic ISMS Documentation Checklist

Prepared by the international community of ISO27k implementers
at www.ISO27001security.com

Version 2.1 12th November 2007

Introduction

This is a collaborative document created by ISO/IEC 27001 and 27002 implementers belonging to the ISO27k implementers' forum. It lists the items typically required to document an Information Security Management System suitable for certification against ISO/IEC 27001.

This checklist is the product of the first phase of a project. A second phase is currently in progress, developing worked examples/samples of the ISMS documents listed on this checklist.

Scope

The checklist simply lists the documents typically produced or used by an ISMS implementation project, plus those produced by and forming part of a mature ISMS.

Purpose

The checklist is meant to help those implementing or planning to implement the ISO/IEC information security management standards. Like the ISO/IEC standards, it is generic and needs to be tailored to your specific requirements. The details do vary between organizations.

Copyright

Disclaimer

This is not a definitive list of ISMS-related documents for all organizations and circumstances. It simply reflects the accumulated experience and knowledge of the contributors of the most common ISMS-related documents. It is merely guidance. Please refer to the ISO/IEC standards and/or consult your accredited ISMS certification body for a more definitive, complete and accurate list.

The Checklist

ISMS Implementation project documents

- ISMS Scope Definition
- ISO/IEC 27002 Questionnaire/Gap Analysis Report
- ISMS Implementation Proposal/Business Case
- ISMS Implementation Plan
- Risk Treatment Plan
- Statement of Applicability
- Information Security Forum approvals/minutes/initiatives
- Risk Assessment Methodology/Approach/Risk Management Strategy
- ISMS Organization (structure chart showing key responsibilities, reporting lines *etc*.)

ISMS Information Security Policies

[Should reference the corresponding sections of ISO/IEC 27002]

- Access Control Policy
- Clear Desk and Clear Screen Policy
- Data Archive And Retention Policy
- Data Classification and Control Policy
- Disposal of Information/Media/Equipment Policy
- eCommerce Security Policy
- Email Security/Acceptable Use Policy
- Information Security Risk Assessment Policy
- IT Outsourcing Security Policy
- Laptop Security Policy
- Mobile Computing and Teleworking Policy
- Overarching ISMS Policy (suggest 1-4 sides maximum *i.e.* a high level management overview and endorsement of the ISMS, a 'superset' of the information security policies)
- Password Policy
- Penetration Testing Policy
- Personnel Security Policy
- Physical Security Policy
- Privacy Policy
- Software Copyright Policy
- Spam Policy
- System/data Backup and Recovery Policy

- System Usage Monitoring Policy
- Third Party Access Policy
- Virus/malware Policy

Baseline technical security standards for …

- Application and other servers
- Databases (*e.g*. Oracle, DB2, Sybase, Access ...)
- Desktops, laptops, PDAs
- Development systems
- DMZ (devices installed in the De-Militarized Zone) including Web servers, email servers and other Internet-exposed systems
- Firewalls
- Mainframes
- Operating systems (*e.g*. Windows XP, Windows 2003, Windows CE, various UNIX, MVS *etc*.)
- Routers and switches
- Test systems
- Third party systems used or installed on-site/on the LAN
- Wired and wireless networks (LAN and WAN, WiFi *etc*.)

Information security-related procedures (process guides)

- Backup Procedure
- Compliance Assessment and Audit Procedures *e.g*. CISCO router security audit procedure
- Incident Reporting Procedure
- Logical Access Review Procedure
- Patch Management Procedure
- Security Admin Procedures (adding user IDs, changing access rights, changing passwords *etc*.)
- System Hardening Procedure
- System Security Testing Procedure
- User Maintenance Procedure

Management system procedures

- Corrective/Preventive Action Procedure
- Document and Record Control Procedure (doc reviews, ownership, management authorization, change controls, reference/"top" copies)
- Internal ISMS Audit Procedure
- Information security guidelines and advisories on various information security topics

- Information Security Awareness Materials (posters, briefings, presentations *etc*. aimed at identified audience groups and topics)

Information security-related job descriptions/rôles and responsibilities

- Information Asset Owner
- Information Security Analyst
- Information Security Architect
- Information Security Manager
- Information Security Officer
- Information Security Tester
- IT Auditor
- Security Administrator

ISMS operational artifacts/records

- Business Continuity Plans (business continuity focused) and Test/Exercise Reports
- Business Impact Assessment Checklist and Reports
- IT Disaster Recovery Plans (IT service restoration focused) and Test/Exercise Reports
- Information Asset Inventory/Database
- Information Security Incident Report Forms and Reports on Significant Incidents
- Review of Solution Design and Architecture Checklist (for software development)
- Threat and Vulnerability Checklists/Questionnaires and Reports

Registers/lists/databases

- Backup and Archive Register (details of tapes/disks, dates, types of backup, scope of backup - possibly automated)
- Business Continuity Plan Register (details of all BCPs showing status, ownership, scope, when last tested *etc*.)
- Standard Desktop Software List (catalog of approved desktop software)
- Information Security Incident Register (may be derived from the IT Help/Service Desk call logging system)
- Privilege/Administrator Access and Authorization List
- Risk Register (risk title, risk owner, nature of risk, management decisions re reduce/transfer/avoid *etc*.)
- Software License Register (supplier, type of license, license conditions/restrictions, owner/manager of vendor relationship)
- System Patch and Antivirus Status Register (likely to be largely automated)
- Third Party Access and Connection Register (showing security information about the links, 3rd parties, contractual information security terms *etc*.)

Notes

The above items, if required by your organization, need to be drafted and reviewed by suitable people, then (for formal documents such as policies at least) approved by management. All versions must be controlled (as per ISO/IEC 27001 section 4.3.2) *e.g.* by ensuring that all approved/current items are uploaded to a controlled area of the intranet, with any superseded versions being removed from that area at the same time. Evidence of the approval status for the documents (*e.g.* committee minutes, approval signatures *etc.*) should be retained by the Information Security Manager, Compliance Officer or equivalent. All documents should be reviewed and if necessary updated every year or two, being careful to update any cross-references.

For reference, ISO/IEC 27001:2005 requires the organization to define and document:

- The **Scope and Boundary** of the ISMS (identified in clause 4.2.1a) and its **Objectives** (4.3.1a);
- An **ISMS Policy** being a superset of the information security policy (4.2.1b);
- A description of the **Risk Assessment Approach** (4.2.1c) or **Methodology** (4.3.1d);
- A **Risk Assessment** or **Risk Analysis Report** identifying information assets in scope of the ISMS, threats to those assets, vulnerabilities that might be exploited by the threats and the impacts that loss of confidentiality, integrity and availability may have, analyzing and evaluating the risks (4.2.1c,d,e,f,g and 4.3.1e);
- The **Risk Treatment Plan** which identifies evaluated options for the treatment of risks (4.2.1f and 4.2.2b);
- **Management Approvals and Authorizations** confirming that management approves the residual risks and authorizes the ISMS (4.2.1h and 4.2.1i);
- The **Statement of Applicability** (4.2.1j) defining the selected control objective and controls along with the reasons they were selected, identifying control objectives and controls currently implemented and documenting the reasons for excluding any control objectives and controls (4.2.1g, drawing on Annex A which summarizes the controls in ISO/IEC 27002);
- **Documented Procedures** to ensure effective planning, operation and control of the security processes, and describe how to measure the effectiveness of the controls (4.3.1g)
- **Records** demonstrating that the ISMS is actually in operation *e.g.* management decisions, outputs of monitoring and review procedures, risk assessments, ISMS audit reports, security plans, occurrences of significant security incidents, visitors' books, completed access authorization forms *etc.* (4.2.3, 4.3.1 and 4.3.3).

References

ISO/IEC 27001 and ISO/IEC 27002 are of course the definitive guides to compliant ISMSs.

Change record

17th Sept 2007: **version 1** released on www.ISO27001security.com. Based on a suggestion and initial list from BalaMurugan Rajagopal, supplemented by inputs from various members of the ISO27k implementers' forum.

10th Nov 2007: **version 2** released with notes on the documentation requirements specified in ISO/IEC 27001 and hyperlinks to the sample documents available on www.ISO27001security.com.

12th Nov 2007: **version 2.1** includes BCP/DR test report records (thanks Shankar).

Feedback

Comments, queries and improvement suggestions (especially improvement suggestions!) are welcome either via the ISO27k implementers' forum or direct to the forum administrator Gary@isect.com