



ISO27k Toolkit Overview and contents

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

[Version 3.2](#) 20th August 2008

Introduction

This document was 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 (ISMS) suitable for certification against ISO/IEC 27001.

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.

The checklist itself is the product of the first phase of a collaborative project to build an **ISO27 toolkit** – a suite of materials to assist those implementing an ISMS using the ISO/IEC 27000-series standards.

The second phase of the project is currently in progress, developing worked examples/samples of the ISMS documents listed on this checklist. Links are provided below to the sample documents already completed and published. Eventually, we hope to complete the toolkit, although it may not make much sense to generate generic samples of *all* the documents listed. If you own examples of other items on the list, or additional examples of those we already have, please submit them to expand the toolkit (contact Gary@isect.com).

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



This work is copyright © 2007, ISO27k implementers' forum, some rights reserved. It is licensed under the [Creative Commons Attribution-NonCommercial-Share Alike 3.0 License](#). You are welcome to reproduce, circulate, use and create derivative works from this *provided* that (a) it is not sold or incorporated into a commercial product, (b) it is properly attributed to the ISO27k implementers' forum (www.ISO27001security.com), and (c) derivative works are shared under the same terms as this.

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: ISO27k Toolkit Contents

ISMS Implementation Project Documents

Documentation supporting the project structure typically set up to implement an ISMS.

- [ISMS Implementation and Certification Process Flowchart](#)
- [ISMS Scope Definition](#)
- ISO/IEC 27002 Questionnaire/Gap Analysis Report
- [ISMS Implementation Proposal \(Generic Business Case\)](#)
- ISMS Implementation Plan
- Risk Treatment Plan (how excessive risks will be mitigated)
- [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.*)
- [Glossary of information security terms](#) (hyperlinked online document)
- [Case Study on an ISMS Implementation](#) outlining the business value of the ISMS
- [ISMS Implementation Guidance and Metrics](#) with hints and tips for implementers
- [Information Security Metrics](#), a sample set to get you thinking

ISMS Information Security Policies

Policy statements covering various aspects of information security. [These should really reference the corresponding sections of ISO/IEC 27002 – that's a loose end.]

- [Overarching ISMS Policy](#) (we suggest no more than 4 sides *i.e.* a high level management overview and endorsement of the ISMS, a 'superset' of the remaining detailed information security policies stating the main principles and objectives of information security)
- Access Control Policy
- Clear Desk and Clear Screen Policy
- Data Archive And Retention Policy
- [Information Classification Policy](#)
- Disposal of Information/Media/Equipment Policy
- eCommerce Security Policy
- [Email Security/Acceptable Use Policy](#)
- Information Security Risk Assessment Policy
- [Laptop Security Policy](#)
- Mobile Computing and Teleworking Policy
- [Outsourcing Security Policy](#)
- 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

Standards specifying security configurations/parameters for various technical platforms.

- 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

Guides to the processes involved in implementing information security controls.

- 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

Guides to the processes involved in managing the ISMS as a whole.

- [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 Awareness Materials (posters, briefings, guidelines, advisories, seminar/training course presentations *etc.* on various information security topics, aimed at identified audience groups)
- [ISMS Auditing Guideline](#)
- [Information Security Risk Analysis Spreadsheet](#) for assessing threats, vulnerabilities and impacts
- [FMEA Risk Analysis Spreadsheet](#) for assessing risks using Failure Modes and Effects Analysis, focusing on potential consequences

Information Security-related Job Descriptions

Rôles and responsibilities, competencies *etc.* for jobs associated with the ISMS.

- [See also the [ISMS Organization](#) listed earlier]
- [Contingency Planning and Disaster Recovery rôles](#)
- 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

Formal records generated as a result of operating the ISMS.

- 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 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

ISMS Registers

Lists or databases of items within the ISMS and information assets.

- 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.*)
- [Information Asset Inventory/Register/Database](#)
- [Information Security Risk Register](#) (risk title, risk owner, nature of risk, management decisions re reduce/transfer/avoid *etc.*)
- Information Security Incident Register (may be derived from the IT Help/Service Desk call logging system)
- Privilege/Administrator Access and Authorization List
- Software License Register (supplier, type of license, license conditions/restrictions, owner/manager of vendor relationship)
- Standard Desktop Software List (catalog of approved desktop software)
- 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 corporate 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 for audit purposes. 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 27001:2005](#) and [ISO/IEC 27002:2005](#) are the definitive guides to compliant ISMSs.

[ISO/IEC 27005:2008](#) provides information on assessing information security risks.

[ISO 27799:2008](#) is the first of several implementation guides aimed at specific industry segments (healthcare in this case).

www.ISO27001security.com offers general advice and guidance on implementing the ISO27k standards, and news on the standards themselves. If you are actually using the standards in anger, join the [ISO27k Implementers' Forum](#) to swap notes with over 1,000 peers and contribute to the continued development of this toolkit.

Document 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).

29th March 2008: **version 3** includes an ISMS Auditing Guideline (thanks all) and Outsourcing Security Policy (thanks Aaron). Added brief introductions to each section of the checklist and turned the bullet points to checkboxes. The document has also been renamed "ISO27k Toolkit - Overview & Contents".

18th May 2008: **version 3.1** links to example high level policy and scope statements (thanks K. Faisal Javed). Various other links updated. If it's not hyperlinked, we probably do not have an example/template available yet. If *you* have one you'd be willing to donate to the toolkit, please get in touch.

20th August 2008: **version 3.2** with links to additional free sample materials provided online.

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