White paper: Checklist of Mandatory Documentation Required by ISO/IEC 27001 (2013 Revision)

27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

WHITE PAPER

September 02, 2014

1. Which documents and records are required?

The list below shows the minimum set of documents and records required by the ISO/IEC 27001 2013 revision:

Documents*	ISO 27001:2013 clause number
Scope of the ISMS	4.3
Information security policy and objectives	5.2, 6.2
Risk assessment and risk treatment methodology	6.1.2
Statement of Applicability	6.1.3 d)
Risk treatment plan	6.1.3 e), 6.2
Risk assessment and risk treatment report	8.2, 8.3
Definition of security roles and responsibilities	A.7.1.2, A.13.2.4
Inventory of assets	A.8.1.1
Acceptable use of assets	A.8.1.3
Access control policy	A.9.1.1
Operating procedures for IT management	A.12.1.1
Secure system engineering principles	A.14.2.5
Supplier security policy	A.15.1.1
Incident management procedure	A.16.1.5
Business continuity procedures	A.17.1.2
Legal, regulatory, and contractual requirements	A.18.1.1

Records*	ISO 27001:2013 clause number
Records of training, skills, experience and qualifications	7.2
Monitoring and measurement results	9.1
Internal audit program	9.2
Results of internal audits	9.2
Results of the management review	9.3
Results of corrective actions	10.1
Logs of user activities, exceptions, and security events	A.12.4.1, A.12.4.3

*Controls from Annex A can be excluded if an organization concludes there are no risks or other requirements which would demand the implementation of a control.

This is by no means a definitive list of documents and records that can be used during the ISO 27001 implementation – the standard allows any other documents to be added to improve the level of information security.

2. Commonly used non-mandatory documents

Other documents that are very often used are the following:

Documents	ISO 27001:2013 clause number
Procedure for document control	7.5
Controls for managing records	7.5
Procedure for internal audit	9.2
Procedure for corrective action	10.1
Bring your own device (BYOD) policy	A.6.2.1
Mobile device and teleworking policy	A.6.2.1
Information classification policy	A.8.2.1, A.8.2.2, A.8.2.3
Password policy	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3

Disposal and destruction policy	A.8.3.2, A.11.2.7
Procedures for working in secure areas	A.11.1.5
Clear desk and clear screen policy	A.11.2.9
Change management policy	A.12.1.2, A.14.2.4
Backup policy	A.12.3.1
Information transfer policy	A.13.2.1, A.13.2.2, A.13.2.3
Business impact analysis	A.17.1.1
Exercising and testing plan	A.17.1.3
Maintenance and review plan	A.17.1.3
Business continuity strategy	A.17.2.1

3. How to structure most common documents and records

Scope of the ISMS

This document is usually rather short, and written at the beginning of the ISO 27 001 implementation. Normally, it is a stand-alone document, although it can be merged into an Information security policy.

Read more here: Problems with defining the scope in ISO 27 001.

Information security policy and objectives

Information security policy is usually a short, top-level document describing the main purpose of the ISMS. Objectives for the ISMS are usually a stand-alone document, but they can also be merged into the Information security policy. Unlike the ISO 27 001 2005 revision, there is no more need for both ISMS Policy and Information security policy – only one Information security policy is needed.

Read more here: Information security policy – how detailed should it be?

Risk assessment and risk treatment methodology & report

Risk assessment and treatment methodology is usually a document of 4 to 5 pages, and it should be written before the risk assessment and risk treatment are performed. The Risk assessment and treatment report has to be written after the risk assessment and risk treatment are performed, and it summarizes all the results.

Read more here: ISO 27 001 risk assessment & treatment – 6 basic steps.

Statement of Applicability

The Statement of Applicability (or SoA) is written based on the results of the risk treatment – this is a central document within the ISMS because it describes not only which controls from Annex A are applicable, but also how they will be implemented, and their current status. You could also consider the Statement of Applicability as a document that describes the security profile of your company.

Read more here: The importance of Statement of Applicability for ISO 27001.

Risk treatment plan

This is basically an action plan on how to implement various controls defined by the SoA – it is developed based on the Statement of Applicability, and is actively used and updated throughout the whole ISMS implementation. Sometimes it can be merged into the project plan.

Read more here: Risk Treatment Plan and risk treatment process – What's the difference?

Security roles and responsibilities

The best method is to describe these throughout all policies and procedures, as precisely as possible. Avoid expressions like "should be done," and instead use something like "CISO will perform xyz every Monday at zxy hours." Some companies prefer to describe security roles and responsibilities in their job descriptions; however, this may lead to lot of paperwork.

Security roles and responsibilities for third parties are defined in contracts.

Read more here: What is the job of Chief Information Security Officer (CISO) in ISO 27001?

Inventory of assets

If you didn't have such an inventory prior to the ISO 27001 project, the best way to create such a document is directly from the result of the risk assessment – during the risk assessment all the assets and their owners must be identified anyway, so you just copy the results from there.

Read more here: How to handle Asset register (Asset inventory) according to ISO 27001.

Acceptable use of assets

This is usually written in the form of a policy, and such a document can cover a very wide range of topics because the standard doesn't define this control very well. Probably the best way to approach it is the following: (1) leave it for the end of your ISMS implementation, and (2) all the areas & controls that you haven't covered with other documents and that concern all employees, cover them with this policy.

Access control policy

In this document, you can cover only the business side of approving access to certain information and systems, or also the technical side of access control; further, you can choose to define rules for only logical access, or also for the physical access. You should write this document only after you finish your risk assessment and risk treatment process.

Operating procedures for IT management

You can write this as a single document, or as a series of policies and procedures – if you are a smaller company, you will tend to have a smaller number of documents. Normally, you can cover all the areas from sections A.12 and A.13 – change management, third-party services, backup, network security, malicious code, disposal and destruction, information transfer, system monitoring, etc. You should write this document only after you finish your risk assessment and risk treatment process.

Read more about IT management here: ITIL & ISO 20000 Blog.

Secure system engineering principles

This is a new control in ISO 27001:2013, and requires that secure engineering principles be documented in the form of a procedure or standard, and should define how to incorporate security techniques in all architecture layers – business, data, applications and technology. These can include input data validation, debugging, techniques for authentication, secure session controls, etc.

Supplier security policy

This is also a new control in ISO 27001:2013, and such policy can cover a wide range of controls – how the screening of potential contractors is done, how the risk assessment of a supplier is made, which security clauses to insert into the contract, how to supervise the fulfillment of contractual security clauses, how to change the contract, how to close the access once the contract is terminated, etc.

Read more here: 6-step process for handling supplier security according to ISO 27001.

Incident management procedure

This is an important procedure which defines how the security weaknesses, events and incidents are reported, classified and handled. This procedure also defines how to learn from information security incidents, so that they can be prevented the next time. Such a procedure can also invoke the Business continuity plan if an incident has caused a lengthy disruption.

Business continuity procedures

These are usually business continuity plans, incident response plans, recovery plans for business side of the organization, and disaster recovery plans (recovery plans for IT infrastructure). These are the best described in the ISO 22301 standard, the leading international standard for business continuity.

To learn more, click here: Business continuity plan: How to structure it according to ISO 22301.

Legal, regulatory, and contractual requirements

This list should be made as early in the project as possible, because many documents will have to be developed according to these inputs. This list should include not only responsibilities for complying with certain requirements, but also the deadlines.

Records of training, skills, experience and qualifications

These records are normally maintained by the human resources department – if you don't have such a department, anyone who usually maintains the employee's records should be doing this job. Basically, a folder with all the documents inserted in it will do.

Read more here: How to perform training & awareness for ISO 27001 and ISO 22301.

Monitoring and measurement results

The easiest way to describe the way controls are to be measured is through policies and procedures which define each control – normally, this description can be written at the end of each document, and such description defines the kinds of KPIs (key performance indicators) that need to be measured for each control or group of controls.

Once this measurement method is in place, you have to perform the measurement accordingly. It is important to report these results regularly to the persons who are in charge of evaluating them.

Read more here: ISO 27001 control objectives – Why are they important?

Internal audit program

The Internal audit program is nothing else but a 1-year plan for performing the audits – for a smaller company this could be only one audit, whereas for a larger organization this could be a series of, e.g., 20 internal audits. This program should define who will perform the audits, methods, audit criteria, etc.

Read more here: How to make an Internal Audit checklist for ISO 27001 / ISO 22301.

Results of internal audits

An internal auditor must produce the Audit report, which includes the audit findings (observations and corrective actions). Such report must be produced within a couple of days after an internal au dit is performed. In some cases the internal auditor will have to check whether all the corrective actions have been performed as expected.

Results of the management review

These records are normally in the form of meeting minutes – they have to include all the materials that were involved at the management meeting, as well as all the decisions that were made. The minutes can be in paper or digital form.

Read more here: Why is management review important for ISO 27001 and ISO 22301?

Results of corrective actions

These are traditionally included in Corrective action forms (CARs). However, it is much better to include such records in some application that is already used in an organization for Help Desk – because corrective actions are nothing but to-do lists with clearly defined responsibilities, tasks and deadlines.

Read more here: Practical use of corrective actions for ISO 27001 and ISO 22301.

Logs of user activities, exceptions, and security events

These are normally kept in two forms: (1) in digital form, automatically or semi-automatically produced as logs of various IT and other systems, and (2) in paper form, where every record is written manually.

Procedure for document control

This is normally a stand-alone procedure, 2 or 3 pages long. If you already implemented some other standard like ISO 9001, ISO 14001, ISO 22301 or similar, you can use the same procedure for all these management systems. Sometimes it is best to write this procedure as the first document in a project.

Read more here: Document management in ISO 27001 & BS 25999-2.

Controls for managing records

The easiest way is to describe the control of records in each policy or procedure (or other document) that requires a record to be created. These controls are normally written toward the end of each document, a nd are usually in the form of a table that describes where the record is archived, who has access, how it is protected, for how long it is archived, etc.

Procedure for internal audit

This is normally a stand-alone procedure that can be 2 to 3 pages long, and has to be written before the internal audit begins. As with the Procedure for document control, one Procedure for internal audit can be used for any management system.

Read more here: Dilemmas with ISO 27001 & BS 25999-2 internal auditors.

Procedures for corrective action

This procedure shouldn't be more than 2 or 3 pages lo ng, and it can be written at the end of the implementation project, although it is better to write it earlier so that employees can get used to it.

4. Sample documentation templates

Here you can download a free preview of the ISO 27001 & ISO 22301 Documentation Toolkit – in this free preview you will be able to see the Table of Contents of each of the mentioned policies and procedures, as well as a few sections from each document.

27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

EPPS Services Ltd.
for electronic business and business consulting
Ul. Vladimira Nazora 59, 10000 Zagreb
Croatia, European Union

Email: support@iso27001standard.com
Phone: +385 1 48 34 120
Phone (for U.S. customers): +1 (646) 797 2744
Fax: +385 1 556 0711