Checklist of Mandatory Documentation Required by ISO/IEC 27001

Advisera

Table of Contents

Which documents and records are required?

The list below shows the minimum set of documents and records required by the ISO/IEC 27001 2022 revision:

What must be documented	ISO 27001 reference	Usually documented through
Scope of the ISMS	Clause 4.3	ISMS Scope document
Information security policy	Clause 5.2	Information Security Policy
Risk assessment and risk treatment process	Clause 6.1.2	Risk Assessment and Treatment Methodology
Statement of Applicability	Clause 6.1.3 d)	Statement of Applicability
Risk treatment plan	Clauseg 6.1.3 e, 6.2, and 8.3	Risk Treatment Plan
Information security objectives	Clause 6.2	List of Security Objectives
Risk assessment and treatment report	Clauses 8.2 and 8.3	Risk Assessment & Treatment Report
Inventory of assets	Control A.5.9*	Inventory of Assets, or List of Assets in the Risk Register
Acceptable use of assets	Control A.5.10*	IT Security Policy
Incident response procedure	Control A.5.26*	Incident Management Procedure
Statutory, regulatory, and contractual requirements	Control A.5.31*	List of Legal, Regulatory, and Contractual Requirements

Security operating procedures for IT management	Control A.5.37*	Security Procedures for IT Department
Definition of security roles and responsibilities	Controls A.6.2. and A.6.6*	Agreements, NDAs, and specifying responsibilities in each security policy and procedure
Definition of security configurations	Control A.8.9*	Security Procedures for IT Department
Secure system engineering principles	Control A.8.27*	Secure Development Policy

*Note: ISO 27001 documents and records required by Annex A controls are mandatory only if there are risks or requirements from interested parties that would demand implementing those controls.

What must be recorded	ISO 27001 reference	Usually recorded through
Training, skills, experience, and qualifications	Clause 7.2	Training certificates and CVs
Monitoring and measurement results	Clause 9.1	Measurement Report
Internal audit program	Clause 9.2	Internal Audit Program
Results of internal audits	Clause 9.2	Internal Audit Report
Results of the management review	Clause 9.3	Management Review Minutes
Results of corrective actions	Clause 10.2	Corrective Action Form
Logs of user activities, exceptions, and security events	Control A.8.15*	Automatic logs in information systems

*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.

Commonly used non-mandatory documents

Other documents that are very often used are the following:

Documents	ISO 27001 clause number
Procedure for Document and Record Control	Clause 7.5, control A.5.33
Procedure for Internal Audit	Clause 9.2
Procedure for Corrective Action	Clause 10.2
Information Classification Policy	Controls A.5.10, A.5.12, and A.5.13
Password Policy	Controls A.5.16, A.5.17, and A.8.5
Supplier Security Policy	Controls A.5.19, A.5.21, A.5.22, and A.5.23
Disaster Recovery Plan	Controls A.5.29, A.5.30, and A.8.14
Mobile Device, Teleworking, and Work from Home Policy	Controls A.6.7, A.7.8, A.7.9, and A.8.1
Procedures for Working in Secure Areas	Controls A.7.4 and A.7.6
Clear Desk and Clear Screen Policy	Control A.7.7
Bring Your Own Device (BYOD) Policy	Controls A.7.8 and A.8.1
Disposal and Destruction Policy	Controls A.7.10, A.7.14, and A.8.10
Backup Policy	A.8.13
Encryption Policy	Control A.8.24
Change Management Policy	Control A.8.32

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 27001 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 27001.

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.

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.

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: Statement of Applicability in ISO 27001 – What is it and why does it matter?

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: ISO 27001 Risk Assessment, Treatment, & Management: The Complete Guide.

Information security specific 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: Asset management according to ISO 27001: How to handle an asset register / asset inventory.

IT security policy

This document is sometimes called an Acceptable Use of Assets Policy. This kind of 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.

Security procedures for IT department

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 technological controls involving things like 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.

Secure development policy

This policy covers secure engineering principles, 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

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 fulfilment 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.

Disaster Recovery plan

These are plans for the recovery of IT infrastructure. These are the best described in the ISO 22301 standard, the leading international standard for business continuity.

To learn more, click here: Disaster recovery vs. business continuity.

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 reports

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: How to perform monitoring and measurement in ISO 27001.

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 would perform the audits, methods, audit criteria, etc.

Read more here: ISO 27001 internal audit: The complete guide.

Internal audits reports

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 audit is performed. In some cases, the internal auditor will have to check whether all the corrective actions have been performed as expected.

Procedure for internal audit

This is normally a stand-alone procedure that can be two to three pages long, and it 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.

You can find more information about the internal audit in this free online training: ISO 27001 Internal Auditor Course.

Management review minutes

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?

Records 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: Complete guide to corrective action vs. preventive action.

Procedures for corrective action

This procedure shouldn't be more than two or three pages long, 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.

For more information, please take a look at this useful handbook: Managing ISO Documentation: A Plain English Guide.

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 and record 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.

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, and 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.

Read more here: How to manage documents according to ISO 27001 and ISO 22301.

You can use this free ISO online tool for handling your documentation, i.e., using it as a document management system (DMS).

Check out ISO 27001 compliance software

To get the templates for all mandatory documents and the most common non-mandatory documents, along with the wizard that helps you fill out those templates, sign up for a free trial of Conformio, the leading ISO 27001 compliance software.

Advisera Expert Solutions Ltd
for electronic business and business consulting

Our offices:
Zavizanska 12, 10000 Zagreb, Croatia
Via Maggio 1 C, Lugano, CH-6900, Switzerland
275 Seventh Ave, 7th Floor, New York, 10001, U.S.

Email: support@advisera.com