

ISO 27001:2022 Documentation



Shelter from the Storm

Checklist & Guide

Documenting and retaining evidence is a vital part of implementing ISO 27001:2022. This guide will take you through the mandated documentation required to achieve certification to the standard. Additionally, it provides helpful advice to consider when creating, structuring and deploying documents and creating the artifacts the standard requires.



The Breakdown

ISO 27001:2022 is broken down into two key areas: the 4-10 clauses, which define the governance aspects and the structure of the standard, and the Annex A controls which, when implemented, will define the controls that you will use to manage risk. Clauses 4 to 10 are a mandatory part of your Information Security Management System (ISMS), you will also need the appropriate supporting documents, artifacts and records. Annex A controls are not mandatory (although most will apply as they are fundamental to running an effective security strategy and not including these would require you to substantiate why you have NOT included them). The ones you do include will need the appropriate policies and evidence, (those pesky artifacts), that the controls selected are effective.

Chief Information Security Officers (CISOs) and Information Security Managers need to understand how the standard is structured and how the clauses and controls are organised. With each clause and subclause, there is a set of guidelines to be followed to achieve compliance. It is important to be mindful of the requirements in terms of policies, processes, activities and documented artifacts.

This checklist is designed to be used as a benchmarking tool to enable you to understand how close (or far) your current suite of documents aligns with ISO 27001. It's also helpful for conducting a gap analysis, responding to customer security questionnaires, or conducting management reviews of your ISMS.

The Required ISO 27001 Documents

If your organisation is intending to gain ISO 27001 certification, these are the required policies, processes and documented evidence, that need to be produced and disseminated to deliver a compliant system.

Operational documents to be used by the security team and key risk stakeholders include:

Clause	Required Documents
4.3	The Scope of the ISMS
5.2	Information Security Policy
6.1.2	Information Security Risk Assessment Process
6.1.3	Statement of Applicability
6.1.3	Information Security Risk Assessment Process
6.2	Information Security Objectives

7.2	Evidence of Competence
7.5.1	Documented Information Necessary for the Effectiveness of the ISMS
8.1	Documented Information Necessary for the Processes of the ISMS
8.2	Results of the Information Security Risk Assessment
8.3	Results of the Information Security Risk Treatment
9.1	Documented Evidence of the Results of Monitoring and Measurement
9.2.2	Documented Evidence of the Audit Programmes and the Audit Results
9.3.3	Documented Evidence of the Results of Management Reviews
9.1	Documented Evidence of the Monitoring and Measurement of Results
9.2	A Documented Internal Audit Process
9.2	Documented Evidence of the Audit Programmes and the Audit Results
9.3	Documented Evidence of the Results of Management Reviews
10.2	Documented Evidence of the Nature of the Non-Conformities and Any Subsequent Actions Taken
10.2	Documented Evidence of the Results of Any Corrective Actions

The Policies

In addition, the following policy statements should be in place. Each policy applies to either all staff or specific functions, i.e. IT, HR, Facilities etc. Whilst some may fit naturally into your information security manual, you may find that certain ones are more appropriate as stand-alone documents. A good example here would be the Acceptable Use Policy. This policy needs to be read and understood by all your employees so it may be more readable as a short but informative document for your employees to read and understand.

Control	Policy
A.5.1	Information security policy and topic-specific policies
A.5.9	Inventory of information and other associated Assets
A.5.10	Policies for the Acceptable use and Procedures for Handling Information and Other Associated Assets
A.5.13	An appropriate set of procedures for information labelling in accordance with the Information Classification Scheme
A.5.14	Information transfer rules, Procedures or Agreements

A.5.18	Topic-specific policy for access control. Including rules for how rights are provisioned, reviewed, modified and removed
A.5.19	Processes and procedures to manage the information security risks associated with the use of supplier's products or Services
A.5.21	Processes and procedures to manage the information security risks associated with the ICT products and services supply chain
A.5.23	Processes for acquisition, use, management and exit from cloud services
A.5.24	Information security incident management processes, roles and responsibilities
A.5.28	Procedures for the identification, collection, acquisition and preservation of evidence
A.5.31	Legal, statutory, regulatory and contractual requirements relevant to information security
A.5.32	Procedures to protect intellectual property rights
A.5.37	Operating procedures for information processing facilities
A.6.2	Employment contractual agreements
A.6.4	A disciplinary process to take action against personnel and other relevant interested parties who have committed an information security policy violation
A.6.6	Confidentiality or Non-Disclosure Agreements
A.8.3	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control (mentioned above in 5.18).
A.8.5	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control (mentioned above in 5.18).
A.8.9	Configurations, including security configurations, of hardware, software, services and networks
A.8.11	Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements (mentioned above in 5.18). taking applicable legislation into consideration
A.8.13	Topic-specific policy on backup
A.8.15	Logs that record Activities, exceptions, faults, and other relevant events
A.8.21	Security mechanisms, service levels and service requirements of network services
A.8.24	Rules for the effective use of cryptography
A.8.25	Rules for the secure development of software and systems
A.8.26	Documented information security requirements that are identified, specified and approved when developing or acquiring applications
A.8.27	Principles for Engineering Secure systems
A.8.29	Security Testing Processes in the development lifecycle

Additional policies or supporting procedures may be required depending on the controls that are included within the Statement of Applicability or the risks that have been identified. For example, if you are a software developer or your organisation develops software you would be expected to have a comprehensive documented Software Development Life Cycle (SDLC) procedure.

Records and artifacts are another important consideration. The operational procedures and policies will need to generate a variety of outputs to demonstrate that they are working and delivering security and business benefits. These artifacts are vital in proving you are actually carrying out the procedures required to maintain compliance with the standard.

Tips for Creating, Structuring and Deploying

The lists provided may look like an awful lot of bureaucracy. Risk Crew advises...to be realistic about the volume of documentation that you reasonably need to create, use, manage and maintain. It's best practice to keep documents and policies down to the minimum at the beginning, as you can always expand to add more later – as your ISMS matures.

Additional Recommendations

1. **Keep policies as simple as possible so that staff can understand and follow them. Each policy should have a succinct:**
 - **Policy Statement** – This should simply state 'what we need to do'
 - **Policy Objective** – Will concisely explain 'why we need to do it'
 - **Policy Owner** – Describes who owns the policy
2. **Create an easy to navigate document hierarchy. For small/medium organisations, Risk Crew recommends the following:**
 - **ISMS Manual** – Contain all operational processes/requirements
 - **Risk Assessment Spreadsheet** – Contain the Asset Inventory, Risk Assessment, Risk Treatment Plan and Statement of Applicability
 - **Acceptable Use Policy** – Contain all policies that apply to all staff
 - **IT Security Policy** – Contain all policies applicable to the IT Department
 - **HR Security Policy** – Contain all policies applicable to the HR Department
 - **Information Security Management Policy** – Contain all policies applicable to the management of security
3. **If you adopt the above hierarchy method...that will cover all your mandated policies and procedures covered within six documents. Here are more tips to keep in mind:**
 - **Writing Techniques** – Policies should be written to align with the culture of the company. Try to avoid making them too academic or technical. Give specific company examples to help bring them to life.
 - **Communication** – You now have developed a fully compliant suite of security policies...great. But they are virtually worthless if they are not communicated to staff. Training in, and awareness of the policies are critical to ensure policies are part of your management toolset.

- **Enforcement** – You now need to ensure that staff are adhering to the policies. One method to consider is appointing departmental ‘policy champions’ whose role is to monitor and educate staff within their area.

How Risk Crew Can Help

Writing and assembling the required documentation can be a gruelling task but it doesn’t have to be. Risk Crew consultants can support you with all your ISO 27001 requirements to help you achieve certification. Risk Crew has been delivering ISO consultancy services for over 30 combined years. Our experts are working practitioners who use their knowledge to accelerate your compliance with the standard.

ISO 27001 Compliance Services

Four services are available – providing you with flexible options to get ISO 27001 working for your organisation. You get the exact amount of expertise and assistance you need to help meet your compliance objectives. Nothing more, nothing less.

Risk Crew also provides **Security Penetration Testing**, we can be your partner in helping you gain ISO compliance and help you stay compliant.

All services are delivered under our 100% satisfaction guarantee.

ISO 27001 Resources

Whether you are just starting your ISO 27001 compliance project or if you're looking to learn more, you're in the right place! Choose from Risk Crew’s complimentary resources and tools.

ISO 27001:2022 Transition Guide

Accelerate your implementation and/or transition with guidance on the updated 2022 standard.

1-2-1 Complimentary Discovery Session

Get a mini-gap assessment and advice from an ISO 27001 expert. Schedule a call or online meeting today.

ISO 27001 Service Overview Brochure

Find out how Risk Crew can help your organisation achieve compliance. Choose from 4 service options to meet your needs.

Let our experts help you
achieve & accelerate your
ISO 27001 Certification.



Shelter from the Storm

Contact us for more information



5 Maltings Place
169 Tower Bridge Road
London SE1 3JB
United Kingdom



information@riskcrew.com
+44 (0) 20 3653 1234
riskcrew.com