**List of mandatory documents required by ISO 27001 (2013 revision)**

If you have ever wondered what documents are mandatory in the 2013 revision of **ISO/IEC 27001**, here is the list you need. Below you will see mandatory documents, and also the most commonly used documents for ISO 27001 implementation.

## Mandatory documents and records required by ISO 27001:2013

Here are the documents you need to produce if you want to be compliant with ISO 27001: (Please note that documents from Annex A are mandatory only if there are risks which would require their implementation.)

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

And here are the mandatory records:

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

## Non-mandatory documents

There are numerous non-mandatory documents that can be used for ISO 27001 implementation, especially for the security controls from Annex A. However, I find these non-mandatory documents to be most commonly used:

* Procedure for document control (clause 7.5)
* Controls for managing records (clause 7.5)
* Procedure for internal audit (clause 9.2)
* Procedure for corrective action (clause 10.1)
* Bring your own device (BYOD) policy (clause A.6.2.1)
* Mobile device and teleworking policy (clause A.6.2.1)
* Information classification policy (clauses A.8.2.1, A.8.2.2, and A.8.2.3)
* Password policy (clauses A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, and A.9.4.3)
* Disposal and destruction policy (clauses A.8.3.2 and A.11.2.7)
* Procedures for working in secure areas (clause A.11.1.5)
* Clear desk and clear screen policy (clause A.11.2.9)
* Change management policy (clauses A.12.1.2 and A.14.2.4)
* Backup policy (clause A.12.3.1)
* Information transfer policy (clauses A.13.2.1, A.13.2.2, and A.13.2.3)
* Business impact analysis (clause A.17.1.1)
* Exercising and testing plan (clause A.17.1.3)
* Maintenance and review plan (clause A.17.1.3)
* Business continuity strategy (clause A.17.2.1)