Mandatory ISMS documentation
required for ISO/IEC 27001 certification

February 2024 Release 2.2

The following 14 types of documentation are *explicitly required* of all certified organisations (as an absolute minimum) in the main body of ISO/IEC 27001:2022.

	Clause	Mandatory documentation
1	4.3	ISMS scope
2	5.2	Information security policy
3	6.1.2	Information security risk assessment procedure
4	6.1.3 (d)	**S**tatement of **A**pplicability
5	6.1.3	Information security risk treatment procedure
6	6.2	Information security objectives
7	7.2	Personnel records
8	*8.1*	*Operational planning and control [see note overleaf]*
9	8.2	Risk assessment reports
10	8.3	**R**isk **T**reatment **P**lan
11	9.1	Security measurements (=metrics!)
12	9.2.2	ISMS internal audit programme and audit reports
13	9.3.3	ISMS management review reports
14	10.1	Records of nonconformities and corrective actions

ISO/IEC 27001 *succinctly* specifies the required "documented information".

Study the standards to understand what that means …

Further guidance is available for ISMS implementers in other ISO27k standards such as ISO/IEC 27002, 27003, 27004 and 27005.

Further guidance is available for certification auditors in ISO/IEC 27006, 27007 and 27008, plus the multipart 17021, as well as the certification body policies, procedures, guidelines *etc*.

Discretionary documentation

The requirement in **Clause 8.1** reads *"Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned."* Strictly speaking, the documented information is discretionary since it is conceivable that someone might gain sufficient confidence *without* the need for *any* written records *e.g.* they could simply observe the processes being performed. However, this seems unlikely in practice, particularly if the clause is referring to the confidence of external parties such as certification auditors, without ready access to observe activities in real time.

The documentation noted in ISO/IEC 27001 Annex A is *only* required *if* your organization deems the associated Annex A controls 'necessary' for your ISMS on the basis of the risk assessment. That means the Annex A controls, and hence the associated documentation, are discretionary from the certification perspective.

Certification auditors typically check that an *audit sample* of your 'necessary' information security processes and controls are operating, requesting and reviewing the associated documentation and records arising. **Documentation is important for management, operational *and* assurance purposes.**

Written records are an obvious way to record whatever your policies and procedures require. If your policies and procedures say something is to be recorded in some form, retain sufficient records as evidence to prove it. Aside from the formal requirements of the standard, do whatever your policies and procedures (and other applicable compliance obligations or conformity requirements) say you should do, or expect to be found not in conformity with ISO/IEC 27001 clauses 4.4 and 8.1.

Change record

Release 1: in 2016, a detailed checklist was prepared by volunteers from the ISO27k Forum, covering both the mandatory and discretionary documentation. It was updated in 2018 and 2022.

Release 2: since nobody has been brave enough to offer to update the 30-page original (!), the checklist was savagely pruned to this succinct 2-pager by Gary Hinson in 2023, now just listing the mandatory documentation. Feedback and corrections are welcome.

Release 2.1 (Jan 2024) was a minor update correcting typos, adding links and clarifying a few points.

Release 2.2 (Feb 2024) added a note clarifying that the clause 8.1 documentation is, strictly speaking, discretionary. Creative Commons license v4 now applies.

Caveat, authorship and copyright

The list could be materially wrong or inadequate to satisfy your auditors, so it comes with no guarantee: it's up to you to check it … and by all means put us completely right.