Mandatory ISMS documentation
required for ISO/IEC 27001 certification

January 2023 Release 2.0

The following documentation is *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	5.1 & 5.2	Information security policy
3	6.1.2	Information security risk assessment procedure
4	6.1.3 (d)	Statement of Applicability
5	6.1.3	Information security risk treatment procedure
6	6.2	Information security objectives
7	7.2	Personnel records
8	8.1	ISMS operational information
9	8.2	Risk assessment reports
10	8.3	Risk Treatment Plan
11	9.1	Security 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 required documentation.

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

Further information is available for certification auditors in ISO/IEC 27006, 27007 and 27008, plus 17021.

Discretionary documentation

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. The Annex A controls, and hence the associated documentation, are discretionary.

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 and manage policies and procedures state. If your policies and procedures say something is recorded in some form, retain sufficient records 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.

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.

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.