Information **S**ecurity **M**anagement **S**ystem

Mandatory and discretionary ISMS documentation

Version	Date	Who	What
1	March 2025	Gary Hinson	Guideline prepared for SecAware ISMS

ISO/IEC 27001:2022 formally requires the following fourteen types of 'documented information':

	Clause	Mandatory items
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 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

documented information
information required to be controlled and maintained by an *organization* (3.50) and the medium on which it is contained

Note 1 to entry: Documented information can be in any format and media and from any source.

Note 2 to entry: Documented information can refer to

— the *management system* (3.41), including related *processes* (3.54);

— information created in order for the *organization* (3.50) to operate (documentation);

— evidence of results achieved (records).

ISO/IEC 27000

Discretionary ISMS documentation

While ISO/IEC 27001 formally 'requires' a minimum of documentation, additional (discretionary) materials can be at least as valuable in practice, and may also be 'required' for certification if needed by the organisation for its ISMS. Two main-body clauses are pertinent.

> ISO/IEC 27001 Annex A control-related documentation is *only* 'required' *if* the associated controls are 'necessary' to mitigate the organisation's unacceptable risks.

ISO/IEC 27001 clause 4.4

> *"The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this document."*

Documentation enables management to inform workers about their responsibilities *e.g.* policies, procedures, rôle descriptions, awareness and training materials such as guidelines and briefings. In addition, many security-related processes generate 'records' such as completed forms, reports and authorisations, useful for assurance, accountability and improvement purposes. Information about the business context, used in planning, scoping and operating the ISMS, should also be retained.

ISO/IEC clause 8.1

> *"Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned."*

In theory someone could be confident without *any* written records, simply by observing the processes being performed. However, a lack of evidence will not satisfy the certification auditors in practice. They typically expect to review *all* the mandatory documentation *and* sufficient discretionary items to confirm that the ISMS conforms with the standard and is operational. With insufficiently-documented audit trails, anticipate major non-conformities against these clauses.

Striking a balance

There is a tendency to go overboard on ISMS documentation, creating reams of red tape. The costs of creating, approving, controlling, using, retaining and maintaining documentation can exceed the business benefits. For example, if the ISMS is too complex and regimented, it will be harder to make improvements and slower to respond to the ever-changing information risks and business needs. It is worth keeping things in check, especially for a new ISMS, by:

- Writing simple, succinct policies and procedures;
- Using plain language and diagrams where appropriate;
- Only formalising activities that truly deserve to be formalised;
- Generating and retaining documentary records only so long as they genuinely add value and are required (*e.g.* personal info);
- Planning to refine the documentation systematically and gradually, taking advantage of experience, feedback and improvement opportunities as the ISMS matures;
- Maintaining a balance between conformity and pragmatism.

> Further guidance is available for ISMS implementers in ISO/IEC 27002, '27003, '27004 and '27005, and for certification auditors in '27006, '27007, '27008 plus the multipart '17021, ISO 19011 and certification body policies *etc*.

In conclusion, an *adequate* blend of mandatory and discretionary items is the key to a business-like, certifiable and sustainable ISMS.