ISO 27001: 2022 Documentation

A quick guide to get you through on the mandated documentation.

ISO 27001 Breakdown

ISO 27001: 2022 is broken down into 2 areas: the mandatory clause from Clause 4 to 10 and the Annex A controls.

Clause 4 to 10 is the governing aspects and forms the backbone of most Management System whereas the Annex A controls what measures you put in place to address the risks.

Since Clause 4 to 10 are a mandatory part of the ISO 27001 Management System, it is therefore a need for appropriate supporting documents and records to available. Whereas for the controls in Annex A, the appropriate policies and its evidence will be mandated depending on the controls that you required, although most of these controls apply.

This quick guide is designed to enable you to benchmark your current suite of documentations that aligned with ISO 27001. You will also find this guide useful for conducting any gap analysis, preparation of any audit including customer audit and checking your readiness for management reviews.

REQUIRED ISO 27001 DOCUMENTS

If your organization is planning for ISO 27001 certification, this section shall provide you a overview of the mandatory documentations (e.g. procedures, policies, records) for a fully compliant system.

Supporting Documents for Clause 4 to 10

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	Evidence of the Results of Monitoring and Measurement
9.2.2	Evidence of the Audit Programmes and the Audit Results

9.3.3	Evidence of the Results of Management Reviews
9.1	Evidence of the Monitoring and Measurement of Results
9.2	A Documented Internal Audit Process
9.2	Evidence of the Audit Programmes and the Audit Results
9.3	Evidence of the Results of Management Reviews
10.2	Evidence of the Nature of the Non-Conformities and Any Subsequent Actions Taken
10.2	Evidence of the Results of Any Corrective Actions

Policies

Clause	Required Documents
A.5.1	Information Security Policy and Topic-Specific Policies
A.5.9	Inventory of Information and Other Associated Assets
A.5.10	Rules For the Acceptable Use and Procedures for Handling Information and Other Associated Assets
A.5.13	An Appropriate Set of Procedures for Information Labelling
A.5.14	Information Transfer Rules, Procedures or Agreements
A.5.18	Topic-Specific Policy on And Rules for Access Control
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	Disciplinary Process
A.6.6	Confidentiality or Non-Disclosure Agreements
A.8.3	Topic-Specific Policy on Access Control
A.8.5	Topic-Specific Policy on Access Control
A.8.9	Configurations, Including Security Configurations, of Hardware, Software, Services and Networks
A.8.11	Topic-Specific Policy on Access Control
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	Information Security Requirements
A.8.27	Principles for Engineering Secure Systems
A.8.29	Security Testing Processes

Additional supporting documents or policies may be required depending on some factors; the activities and services, the compliance needs for applicable legislation, customer's contractual requirements, etc.

Take for example, a company that is application developer maybe be expected to have a Software Development Life Cycle (SDLC) procedure.

Records are a vital part of any compliant management system demonstrating the outputs of the operational procedures and policies.

How to create, structure and deploy your documents

This quick guide may seem overwhelm for any organization that is planning for ISO 27001 certification. What we can advise at G.E.N.S is that organization have to be realistic on the reasonable documentation that need to be created, used and maintained. It is always good to keep documentations and policies to a minimum and building your documented system as your management system matures.

Tips and good practices

1. Always keep policies as simple as possible so that every user, staff is able to understand and follow them. Each policy shall be clear and short; expressing what needs to be said without unnecessary words:
   - Policy statement – This should simply state "What we need to do"
   - Policy objective – Provide clear description "Why we need to do"

2. Create a hierarchy structure of your documented system, if possible:
   - ISMS Manual – Document all operational processes, requirements including any policy commitment, objectives. Use annexes to further elaborate key points if required.
   - Risk Assessment Spreadsheet – Document the Asset Inventory, Risk Assessment, Risk Treatment Plan and Statement of Applicability in various tabs of the spreadsheet
   - 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 Manager Policy – Contain all governing policies applicable to the management of security

3. Do also take note of the following:
   - Writing Techniques – Avoid creating policies that are too academic or technical. Use real operation tasks as example which align with the organization context.
   - Communication – Communicate these policies to the staffs for awareness and guiding purpose, else whatever policies created will be worthless.
   - Enforcement – Enforce the implementation and rules of these policies thru regular audit, appointing personnel across functional levels to monitor, guide and educate the staff.

How G.E.N.S can help you

Over at G.E.N.S, we understand that creating any documentation is a demanding and tiring task and we can fully aid your organization in the journey towards ISO 27001 certification. G.E.N.S has been delivering ISO consultancy services since 2013. Our consultants are well equipped with the required industrial knowledge and expertise to further accelerate your compliance with the Standard.

Contact us for more information


www.gensmgt.com


engsoon@gensmgt.com


11 Collyer Quay #14-09 The Arcade Singapore 049317


Mobile: +65 96898369
Tele: +65 64578830