

Integration Guide for ISO 27001:2022 Into an ISO Based OHSMS

This integration guide provides direction and advice for an organization that is integrating these standards:

- ISO 27001:2022 Information Security Management Standard, (or ISMS)
- ISO 45001:2018 Occupational Health and Safety Management Standard (or OHSMS)

Here are supporting items in adding an ISMS to an OHSMS:

- 1-Integration Instructions ISMS into OHSMS Integration.pdf (this document)
- 2-Document Guide ISMS into OHSMS.pdf ... This is a visual representation of necessary changes.
- 3-ISMS-Docs-Flowdown-Matrix-27001+OHSMS
- 4-Style-Guide-Standards Stores
- OHSMS Guidance: ISO 45001 OHSMS Requirements
- Additional information on integrating standards



ISMS Integration into an OHSMS System

1.1 ISMS Documentation

Standards Stores documents are referenced, which will make it easier for those organizations who have purchased documentation from The Standards Stores. [You will see Standards Stores document numbers referenced in parentheses – (SS:X-yyy)]. However, it is not necessary. If your organization used other document packages, or developed your OHSMS internally, the references in this guide may still align with your existing processes, documentation, and work products.

Be sure to use document '2-Document Guide ISMS into OHSMS.pdf'

1.2 Major Changes when Adding ISMS

It is not entirely accurate to describe “major changes” when adding an ISMS to an existing OHSMS. That is because all differences between ISMS and OHSMS must be acknowledged and addressed, especially if your organization plans to seek certification. As such, all changes or differences are “major” in that perspective.

In practice, however, it is possible to give emphasis to significant differences between ISMS and OHSMS, which represent major changes that your organization will need to implement. For an existing OHSMS system, the following ISMS documentation (and associated processes) must be added because they are not covered in your OHSMS:

1.2.1 Critical Processes

These two ISO 27001 processes are of heightened importance:

- Risk Management
- Statement of Applicability (SoA)

Both processes must be documented.

1.2.1.1 Risk Management

Risk management is a fundamental process required by ISO 27001. ISMS section 6 addresses planning a risk management process (risks and opportunities, risk assessment, risk treatment, and information security risk management). ISMS section 8 addresses implementation of risk management planning, including risk assessment activities, risk treatment, and risk reporting.

Risk planning is addressed in ISO 45001. However, it is primarily addressed in OHSMS section 6 as a planning requirement. It is addressed in section 8 as follows: section 8.1.2 addresses “eliminating hazards and reducing OH&S risks.” OHSMS section 8 does not require organizational risk treatment and risk reporting. For OHSMS, an organization only needs to consider “reduction of OH&S risks”

To add ISMS to an existing OHSMS, an organization must implement a full, robust, and active risk management process. That can be achieved by implementing a risk management plan and supporting work products, including a risk register. The risk management process is documented by:

- Risk Management Plan (SS: P-600)
- Risk Register (SS: F-800)
- Risk Register Work Instruction (SS: WI-800)

ISO 27001 (ISMS) Bolt-on to an Existing ISO 45001 (OHSMS) System			
Applicable Clause	Document	Why it is needed for an OHSMS System	Notes and Comments
8	P-801	This ISMS document is bolted onto an existing OHSMS system in order to comply with ISMS operational requirements (Data Classification).	
9	F-905	This ISMS document is bolted onto an existing OHSMS system in order to comply with ISMS management review requirements.	Management review forms may be incorporated into existing OHSMS documentation as long as all ISMS inputs and outputs are addressed.

SAMPLE

4.3 List of Figures

Our documentation does not pre-populate a list of figures. An organization may insert a list of figures (when applicable or if desired) utilizing standard Microsoft table insertion capabilities. Organizational Obligations

4.4 Blue Text

Documentation packages utilize blue text in locations where the organization is responsible to add, insert, edit, or delete specific data or information. Several common examples include:

Location where an organization may insert a logo

Location where an organization may identify process application

Approval name and title

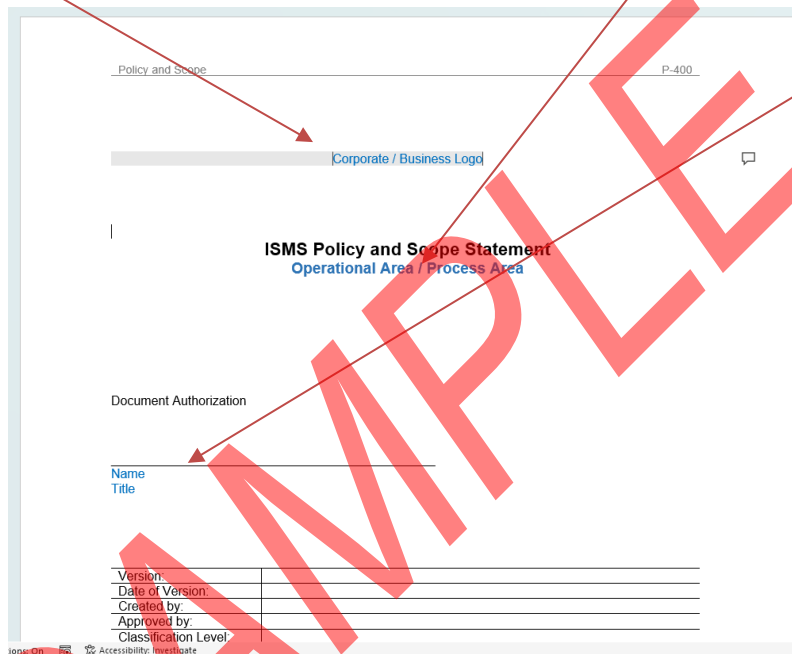


Figure 1 – Examples of Blue Text

It is highly recommended that organizations either address or change blue text before implementation.

An organization is not limited to changing only blue text.

4.4.1 Your Organization / Appropriate Role

The two most common blue text terms in the documentation are:

1. **Your Company:** Substitute your business or company name or preferred abbreviation at each location where **Your Company** is found in a document.
2. **Appropriate Role:** Evaluate, determine, and then insert the proper role or position within your company or business at each location where **Appropriate Role** is found in a document.



Information Security / Information Technology Policy

Operational Area / Process Area

Document Authorization

Name
Title

Version:	
Date of Version:	
Created by:	
Approved by:	
Classification Level:	

SAMPLE

Table of Contents

1. PURPOSE, SCOPE AND USERS	3
1.1. PURPOSE.....	3
1.2. SCOPE.....	3
1.3. USERS.....	3
2. RESPONSIBILITIES AND AUTHORITIES	3
3. REFERENCE DOCUMENTS	3
3.1. REFERENCES	3
4. COMPUTERS, LAPTOPS, MOBILE DEVICES	3
5. VIRUS PROTECTION POLICY	4
6. PASSWORD POLICY	4
7. INTERNET ACCESS POLICY	5
8. ACCESS MANAGEMENT POLICY	7
9. ACCEPTABLE USE	8
10. SYSTEM DEVELOPMENT, IMPLEMENTATION, AND CHANGE CONTROL	9
11. BACKUP POLICY	9
12. RECOVERY POLICY	9
13. CRYPTOGRAPHIC CONTROLS	9
14. CONTROL OVER INSTALLATION OF SOFTWARE	10
15. RELEVANT CONTACTS	10
16. THREAT REPORTING	11
16.1. SECURITY THREAT.....	11
16.2. SECURITY EVENT.....	11
17. INFORMATION TRANSFER CONTROL	11
17.1. DATA CLASSIFICATION	12
17.2. EMAIL TRANSFER	12
17.3. ELECTRONIC DATA TRANSFER / UPLOADING	12
17.4. REMOVABLE DRIVES.....	12
17.5. PHYSICAL DELIVERY	12
18. OPPORTUNITIES AND RISKS	12
19. APPENDICES	12
20. CHANGE HISTORY	14

1. Purpose, Scope and Users

1.1. Purpose

This procedure establishes policies for control over information and data systems compliant with Information Security Management System (ISMS) requirements.

1.2. Scope

The procedure addresses Information Security (IS) and Information Technology (IT) policy, as necessary to meet ISMS objectives.

1.3. Users

This document applies to all **Your Company** personnel and relevant external parties, including external providers who become obligated to adhere to this procedure by agreement with **Your Company**.

2. Responsibilities and Authorities

It is the responsibility of all personnel and employees of **Your Company** to implement and maintain the requirements of this procedure. It is the responsibility of all personnel to effectively communicate the requirements of this procedure (internal communication) to applicable functional groups, support teams, and other personnel involved in the effective implementation and continual improvement of the ISMS.

The **Appropriate Role** has primary responsibility and approval authority for this procedure, including any changes, amendments, or updates.

3. Reference Documents

3.1. References

- This document addresses Annex A of the ISO 27001:2022 standard (Controls and Control Objectives).
- Specific Annex A controls are identified under each section of this procedure.
- P-801 (Data Classification)
- F-602 (Relevant Contacts)

4. Computers, Laptops, Mobile Devices

Computer workstations, laptops, machines, or other company assets are provided to fulfil job functions. Computer workstations, laptops, machines, or other company assets are the property of the company and fall under all applicable policies. All personnel are required to follow these policies and procedures, as well as all other company directives.

All computer-related devices must be ordered in accordance with organizational asset purchasing and control.

Company assets will be tracked using tools and capabilities selected by the organization from time-to-time.

Organizational assets may be named and labelled, including asset tags.

All computer-related devices will be inventoried by the organization.

No personnel shall leave a device or asset logged in and the screen unlocked when left unattended.

Use of employee-owned personal computing devices is not permitted to access company systems without prior advanced approval.

The use of bring your own device (BYOD) is permitted, however all company IT policies must be followed before devices can directly access company resources.

This section supports the following controls:

- Control A.5.13 (asset labeling); refer to P-801 for data and information labeling.
- Control A.5.15
- Control A.8.1

5. Virus Protection Policy

All managed computer devices have virus and malware protection software installed, when applicable. This software has been configured to identify and download any new signatures or database files and perform system scans. Scans are an automated process – personnel are not permitted to tamper with or disable scans or scanning software. This policy applies to all employees, personnel, contractors, and systems.

All systems commonly affected by viruses must have active and current virus scanning software.

Personnel who believe that they have received a virus via any means must immediately contact the IT team or report issues to a supervisor.

Virus software will check for updates of current virus pattern or signature files on a regular basis.

Audits of servers, desktops, workstations, and laptops may be performed at any time to confirm that virus protection is enabled, operational, and using up-to-date pattern or signature files.

Upon virus detection that is not automatically resolved by antivirus software, the machine(s) must be removed from operation immediately. Notify your supervisor so the machine can be cleaned or reimaged before being placed back into service.

This section supports the following controls:

- Control A.8.7

6. Password Policy

Passwords are not to be written down or displayed in public viewable locations.

No personnel shall share or otherwise disclose their password with other parties, including technology staff. Passwords which have been disclosed must be immediately changed or reset. Passwords are not to be disclosed to anyone, under any circumstances, except temporary passwords provided by IT during orientation and/or a user request. Any temporary passwords provided by IT must be changed at the next login.