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

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 14001:2015 Environmental Management Standard (or EMS)

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

- 1-Integration Instructions ISMS into EMS Integration.pdf (this document)
- 2-Document Guide ISMS into EMS.pdf … This is a visual representation of necessary changes.
- 3-ISMS-Docs-Flowdown-Matrix-27001+EMS
- 4-Style-Guide-Standards Stores
- EMS Guidance: ISO 14001 EMS Requirements
- Additional information on integrating standards

ISMS Integration into an EMS 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 EMS 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 EMS.pdf'

1.2 Major Changes when Adding ISMS

It is not entirely accurate to describe "major changes" when adding an ISMS to an existing EMS. That is because all differences between ISMS and EMS 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 EMS, which represent major changes that your organization will need to implement. For an existing EMS system, the following ISMS documentation (and associated processes) must be added because they are not covered in your EMS:

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 14001. However, it is only addressed in EMS section 6, not in section 8. For EMS, an organization only needs to consider risk issues when planning its EMS. There is no requirement for execution of risk assessment, risk treatment, risk reporting, etc.

To add ISMS to an existing EMS, 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 14001 (EMS) System			
Applicable Clause	**Document**	**Why it is needed for the EMS System**	**Notes and Comments**
4	P-400	ISMS procedure P-400 is bolted onto an existing EMS system to define IS policy, and the scope and boundaries of information and data security. Adds ISMS / security (1) policy and (2) objectives to an existing EMS system.	It is possible to incorporate this document into an existing EMS Manual or EMS organizational context procedure.
5	P-500	This ISMS procedure is bolted onto an existing EMS system because ISMS and EMS leadership requirements are sufficiently different that this procedure is necessary to address gaps.	It is possible to incorporate this document into an existing EMS leadership procedure. If combined, ensure that all ISMS leadership requirements are covered in the combined procedure.

4.3 List of Figures

Our documentation does not pre-populate a list of figures. An organization may insert a list of figures (when appliable 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

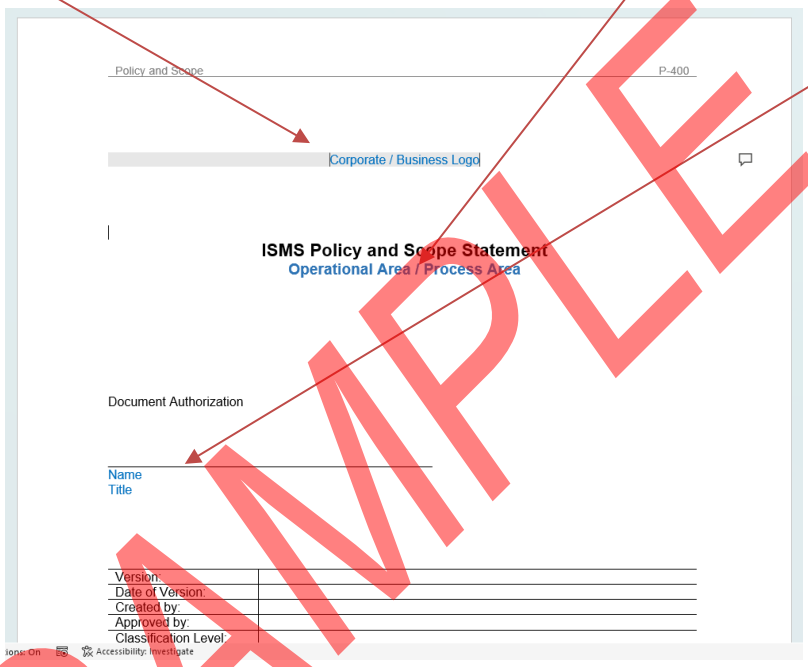

Figure 1 – Examples of Blue Text

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:	

Table of Contents

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.