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

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 9001:2015 based Quality Management Standard (or QMS) like:
  - AS9100/AS9110/AS9120
  - IATF 16949
  - ISO 13485, etc

Here are the critical supporting items in adding an ISMS to a QMS:

- 1-Integration Instructions ISMS into QMS Integration.pdf (this document)
- 2-Document Guide ISMS into QMS.pdf … This is a visual representation of necessary changes.
- 3-IMS-Docs-Flowdown-Matrix-27001+9001
- 4-Style-Guide-Standards Stores
- QMS Guidance: ISO 9001 QMS Requirements
- **Guidance on adding an ISMS to a QMS**: Integration of ISMS to ISO QMS
- Additional information on integrating standards

SMS Integration into a QMS 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 QMS 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 QMS.pdf'

1.2 Major Changes when Adding ISMS

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

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 9001. However, it is only addressed in QMS section 6, not in section 8. For QMS, an organization only needs to consider risk issues when planning its QMS. There is no requirement for execution of risk assessment, risk treatment, risk reporting, etc.

To add ISMS to an existing QMS, an organization must implement a full, robust, and active risk management process. That can be achieved by implementing 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)

Includes a detailed guide which provides clause by clause guidance about where to make changes to your QMS to include 27001:2022 ISMS

ISO 27001 (ISMS) Bolt-on to an Existing ISO 9001 (QMS) System				
Applicable Clause	**Document**	**Title / Process**	**Why it is needed for the QMS System**	**Notes and Comments**
4.3 5.1 5.2	P-400	Policy and Scope Statement	ISMS procedure P-400 is bolted onto an existing QMS 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 QMS system.	It is possible to incorporate this document into an existing QMS Quality Manual.
6	F-600	Asset List	ISMS Form F-600 is bolted onto an existing QMS system to fulfill asset identification and management requirements.	

1. Purpose, Scope and Users

1.1. Purpose

This procedure establishes a security incident response process compliant with Information Security Management System (ISMS) requirements. The security incident response process is also applicable to the organization's Quality Management System (QMS).

1.2. Scope

The procedure addresses security incident response, as required 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 section 6 of the ISO 27001:2022 standard (Planning).
- This document addresses section 8 of the ISO 27001:2022 standard (Operations).
- This document addresses Control A.5.24 of the ISO 27001:2022 standard (Information Security Incident Management Planning and Preparation).
- This document addresses Control A.5.25 of the ISO 27001:2022 standard (Assessment and Decision on Information Security Events).
- This document addresses Control A.5.26 of the ISO 27001:2022 standard (Response to Information Security Incidents).
- This document addresses Control A.5.27 of the ISO 27001:2022 standard (Learning from Information Security Incidents).
- This document addresses Control A.5.28 of the ISO 27001:2022 standard (Collection of Evidence).

4. Security Incident Response Plan

This procedure provides personnel with guidelines for handling information security incidents. The primary audience is Your Company personnel. However, other interested parties may include customers, external providers, and law enforcement.

The term incident in this document means a data security occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

This procedure outlines the need to be prepared before an incident occurs. In this regard, incident management is an aspect of risk management (refer to procedure P-600). This includes having tools and supplies ready as well as having knowledge of computer law and digital evidence gathering and handling.

The purpose of this procedure is not to deal with every conceivable incident or possible technical response. Rather, the purpose is to provide guidelines for a systematic response and point to more technical and human resources where needed.

4.1. Security Incident Response Policy

The following policy is part of this Security Incident Response Plan.

No party involved in a security incident is permitted to publicly discuss information associated with ongoing privacy or security investigations. Disclosures of any kind not formally authorized by Your Company leadership may impede law enforcement efforts.

Personnel shall be mindful of their obligations to maintain confidentiality and remember that only designated personnel are authorized to represent the company in an incident situation.

Personnel shall protect and maintain the integrity of all evidence related to privacy and security incidents. All incident related information, data, and devices are subject to inspection, audit, and review if deemed necessary.

Personnel shall immediately report privacy and security incidents to Appropriate Role.

Reportable privacy and security incidents include, but are not limited to:

- Theft, fraud, data breach, data release, service interruption, or physical intrusions

Violations to privacy, security, or business conduct policies include:

- Malicious activity or any misconduct resulting in the reduced ability to ensure the privacy or security of information.
- Activities which are unfair, deceptive, or unethical.
- Unauthorized access to, or disclosure of, any confidential information.
- Vulnerabilities or threats associated with the integrity or effectiveness of privacy or security controls.
- Social engineering attacks including but not limited to phishing or vishing.
- Any unauthorized system access or probes which have occurred.
- Unauthorized computer activity including but not limited to:
  - Improper password usage or password loss
  - Denial of service

7. Change History

Version	Date	Created by:	Description of Change
v1	enter date	enter name	Initial release of document.