Documentation Style Guide for ISO 27001:2022

This style guide serves two (2) primary purposes:

1. Explains how to use the Standards Stores documentation toolkit you have purchased.
2. Provides document style guidance that is applied to Standards Stores documentation you have purchased.

As you edit Standards Stores documentation, utilizing style guide information will ensure your documents and changes are consistent.

Table of Contents

Figures

8 Application of ISO 27001

This section of the Style Guide provides specific information about your ISO 27001 toolkit.

8.1 Critical Processes

Arguably, all required ISO processes are critical, especially if your organization seeks to become ISO certified. Your Standards Stores toolkit should allow you to implement processes that conform to ISO 27001.

Two ISO 27001 processes are of heightened importance. Those two processes are:

- Risk Management
- Statement of Applicability (SoA)

Both processes must be documented.

8.1.1 Risk Management

The risk management process is documented by:

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

The Risk Management Plan explains risk management implementation within your organization. Review the Risk Management Plan and implement its guidance. If you elect to alter the Standards Stores Risk Management Plan, consider possible impacts upon related documents of F-800 (Risk Register) and WI-800 (Risk Register Work Instruction).

By implementing the Risk Register (F-800), and following the Risk Management Plan, your organization will conform to ISO 27001 Section 6 (Planning) and Section 8 (Operation).

WI-800 (Risk Register Work Instruction) provides step-by-step instructions on how to use the Risk Register (F-800).

8.1.2 Statement of Applicability (SoA)

The Statement of Applicability (SoA) is a unique document. It is primarily applicable to Information Security (IS) and Information Technology (IT) business environments. It is required for Information Security Management Systems (ISMS / ISO 27001).

The SoA requires that your organization review each mandatory control. As you review each control, determine whether the control is applicable to your organization. If a control is not applicable, use the SoA to identify the control as Not Applicable, and provide an explanation as to why it is not applicable.

If a control is applicable, use the SoA to identify the control as Applicable, and explain how your organization addresses and fulfills the control requirement.

Any text may be edited. Blue text provides examples of what you may want to use. Black text is text that describes document as developed by Standards-Stores.com

Corporate / Business Logo

ISMS Policy and Scope Statement

Operational Area / Process Area

Blue text throughout the manual highlight areas for customization

Document Authorization

Name
Title

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

Table of Contents creates a simple snapshot of heading throughout your document.

Table of Contents

You can search and replace "Your Company" with your own company name.

7. ISMS Objectives and Corresponding KPIs

Your Company establishes ISMS objectives which are evaluated by Key Performance Indicators (KPIs).

ISMS Objective	Primary Responsibility	Measures	When it is Completed
Information and data are protected against unauthorized access	Appropriate Role	Security Breach KPI Enforcement Reporting KPI	Continual activity Security Breach KPI is measured monthly Enforcement Reporting KPI measured based upon incident
Confidentiality of information and data is maintained	Appropriate Role	Security Breach KPI Enforcement Reporting KPI	Continual activity Security Breach KPI is measured monthly Enforcement Reporting KPI measured based upon incident Incident Response Plan is implemented
Information is not disclosed to unauthorized persons through deliberate or careless action	Appropriate Role	Security Breach KPI Enforcement Reporting KPI Risk Report KPI	Continual activity Security Breach KPI is measured monthly Enforcement Reporting KPI measured based upon incident Risk Report KPI is measured monthly
The integrity of information and data through protection from unauthorized access or modification	Appropriate Role	Risk Register Risk Report KPI	Continual activity Reported monthly
Commitment to continual improvement where risks are identified, analyzed, and treated	Appropriate Role	Risk Report KPI CIP Implementation KPI	Continual activity KPI is measured monthly
Any breach of information security or suspected weakness is reported and thoroughly investigated	Appropriate Role	Security Breach KPI Enforcement Reporting KPI Risk Report KPI	Continual activity Security Breach KPI is measured monthly Enforcement Reporting KPI measured based upon incident

			Incident Response Plan is implemented

8. Key Parties and Requirements

Your Company evaluates and determines its key parties relative to the ISMS and their significant requirements. Key interested parties and requirements are described in the table below.

Key Interested Party	Interested Party Representative	Significant Requirements	Key Point of Contact
Employees / Personnel Blue text gives guidance for customization.	If there are unions or employee representatives, they are identified here. If not, suggested language is “Not Applicable, personnel represent themselves”	Protection of personal / personnel data (PII) from vulnerabilities. Physical protection(s)	Personnel: Identify unions or employee representatives (if applicable) or say Individual employees represent themselves Your Company: Human Resources Manager or other Appropriate Role
Customer	Customer Representatives (as applicable to each customer)	Contractual requirements	Customer Representatives (as applicable to each customer)
External providers (vendors and suppliers)	Varies (often a sales representative)	Payment for goods or services, and associated requirements	External Providers: Sales Representative Your Company: Appropriate Role

9. Process Architecture

Your Company has developed and implemented a process architecture as a means of structural design, understanding (organizational knowledge), and representation of its key processes and their interrelationships.

The process architecture should be considered dynamically as both process infrastructure and interactions. The process architecture describes key process components and their interactions. The process architecture helps outline organizational processes, communicate key activities internally and externally, and allows for continual improvement of the organization’s ISMS. The process architecture is displayed in the figure below.

Documents are in Microsoft Word for ease of editing

Corporate / Business Logo

Work Instructions are intended to provide specific guidance, direction, or step-by-step instructions to accomplish a task.

Statement of Applicability (SoA) Work Instruction

Operational Area / Process Area

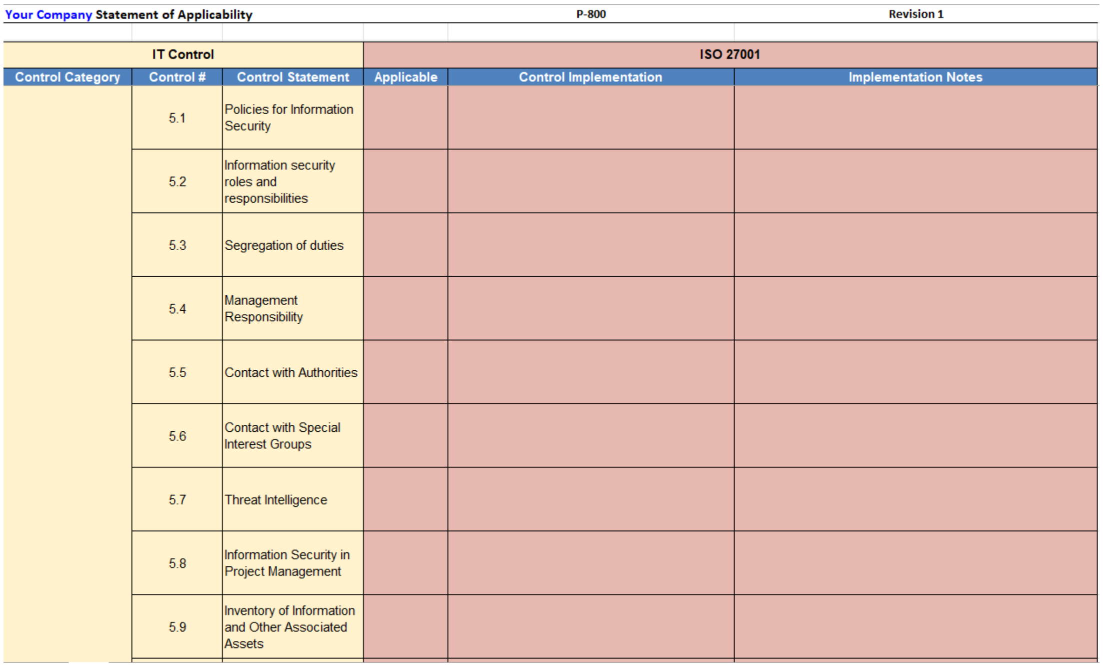
Document Authorization

____

Name
Title

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

Included work instructions show detailed instructions.



Your Company Statement of Applicability P-800 Revision 1

IT Control			ISO 27001		
Control Category	Control #	Control Statement	Applicable	Control Implementation	Implementation Notes
	5.1	Policies for Information Security			
	5.2	Information security roles and responsibilities			
	5.3	Segregation of duties			
	5.4	Management Responsibility			
	5.5	Contact with Authorities			
	5.6	Contact with Special Interest Groups			
	5.7	Threat Intelligence			
	5.8	Information Security in Project Management			
	5.9	Inventory of Information and Other Associated Assets			

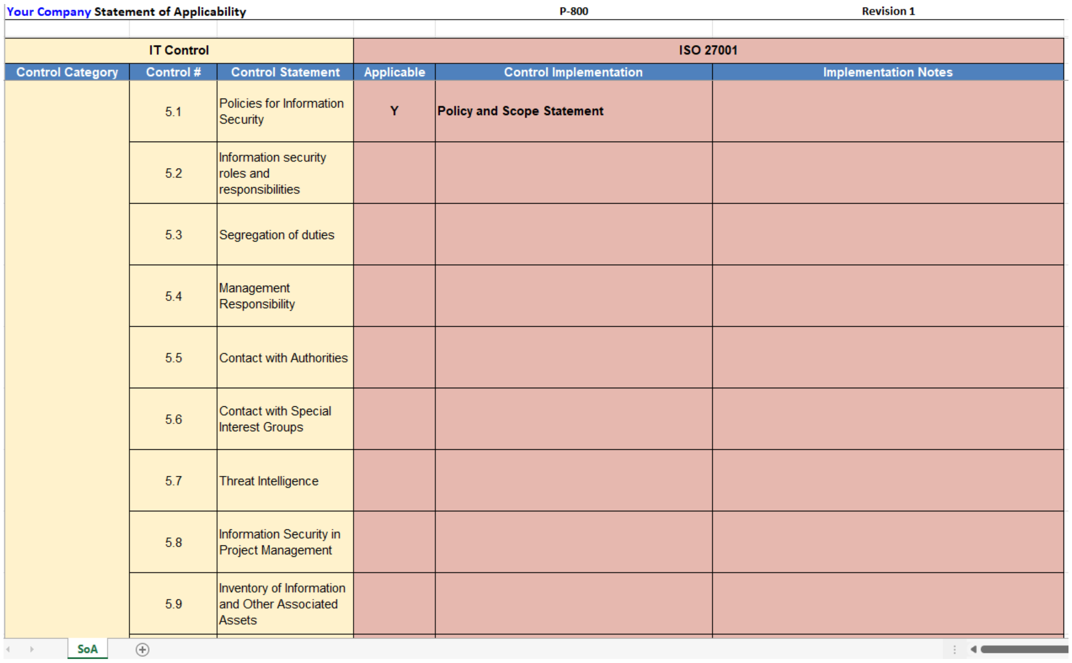
4.1.5. *Control Implementation*

The control implementation column is the fifth column of the SoA (as displayed above).

When preparing or updating the SoA, enter information into this column that evidences how Your Company has implemented this control requirement.

In the diagram below, the SoA is displayed and control 5.1 (Policies for Information Security) has been marked with a Y (for Yes) as an example

In addition, sample language has been entered into the control implementation column indicating that the organization implements this control by instituting an ISMS Policy and Scope Statement.



Your Company Statement of Applicability P-800 Revision 1

IT Control			ISO 27001		
Control Category	Control #	Control Statement	Applicable	Control Implementation	Implementation Notes
	5.1	Policies for Information Security	Y	**Policy and Scope Statement**	
	5.2	Information security roles and responsibilities			
	5.3	Segregation of duties			
	5.4	Management Responsibility			
	5.5	Contact with Authorities			
	5.6	Contact with Special Interest Groups			
	5.7	Threat Intelligence			
	5.8	Information Security in Project Management			
	5.9	Inventory of Information and Other Associated Assets			