COMPANY document template instructions

This COMPANY document template represents a compliance-ready document with placeholders for company-specific text. Each document section represents a topic that you should consider and/or modify to match your company’s practices.

For each document section

* Consider if this section applies to you. If it does not, remove it and/or replace it with your organization’s corresponding practices.
* Replace any highlighted text in angled brackets < > with your own language
* Rewrite the document language such that it reflects the practices of your organization

Document completion checklist

1. Use Find to make sure that all text in angled brackets is replaced
2. Proofread your document for spelling and grammar mistakes
3. Confirm that the document’s content reflects your organization’s practices
4. Add any company-specific letterhead, branding, and formatting
5. Remove this instructions page
6. Export this document as PDF — File > Save As > Change “File Format” to PDF
7. Upload the PDF to COMPANY at https://app.COMPANY.com/policies

More questions?

A good rule-of-thumb is to keep your language high enough level such that it stays representative for at least a year. If you have more questions about how to use this template, please reach out to your Customer Success Manager or your auditor for additional guidance.

Document Name: Risk Assessment and Risk Treatment Process

Document Number: 04-ISMS

| Company Name: | <Company Name> |
| --- | --- |
| Policy Owner(s): | <Policy owner(s)> |
| Effective Date: | <Effective date> |

# Purpose

The purpose of the Risk Assessment and Risk Treatment process is to assess risks to the achievement of <Company Name>’s information security and business objectives.

# Policy

Information security risks and risk treatments shall be managed in accordance with the <Company Name> Risk Management Policy.

# Statement of Applicability (SoA)

The Statement of Applicability will document the controls that have been selected from Annex A of the ISO/IEC 27001 (“ISO 27001”) Information Security standard and the reasons for their selection or exclusion.

# Management Approval

The ISMS Governance Council will be presented with the Statement of Applicability (“SoA”) and highlights from the risk assessment as determined by the Information Security Management Leader. The entire SoA and risk assessment report shall be made available to the ISMS Governance Council members upon request.

ISMS Governance Council may provide feedback on the risk management process to management during the annual management review or as needed at the discretion of the ISMS Governance Council.

Unless explicit input is received from the ISMS Governance Council regarding the SoA or Risk Assessment, the SoA and all risk treatment plans shall be considered acceptable and approved by the ISMS Governance Council following the Management Review.

# Maintenance and Criteria for Performing Risk Assessments

A Risk Assessment will be performed at least <frequency of Risk Assessment, e.g., annually> or may be carried out under the following circumstances with varying scopes as determined by the Information Security Management Leader. Additionally, risks may be assessed at various levels of the organization for circumstances that include:

* Risks to the achievement of the objectives of the ISMS
* Potential for the loss of confidentiality, integrity or availability of customer or company data
* As part of projects that involve significant change to the organization, the ISMS, or the organization’s assets
* Software development, technology, and organizational changes
* When third-party suppliers are engaged, changed, or periodically during the relationship
* In response to significant external changes affecting the organization which may invalidate the conclusions from previous Risk Assessments, e.g., changes to relevant legislation

Risk Assessments may be carried out as a result of other circumstances at the discretion of the Information Security Management Leader or ISMS Governance Council.

# ISO 27001 Coverage

ISO 27001 6.1.1; 6.1.2; 6.1.3

# Version History

| **Version** | **Date** | **Description** | **Author** | **Approved by** |
| --- | --- | --- | --- | --- |
| <1.0> | <Date of change> | Initial policy | <Author of changes> | <Approver of changes> |
|  |  |  |  |  |
|  |  |  |  |  |

# 27701 Privacy Information Management System (PIMS) Addendum

This addendum is automatically applicable for organizations implementing ISO 27701 and optional for organizations who are implementing ISO 27001 only.

* All references to “ISMS” in this document are changed to “IS&PMS”
* All references is ISO 27001 in this document are changed to “ISO 27001/27701”
* All references to “information security management system” are changed to “information security and privacy management system”