[organization logo]

[organization name]

**PROJECT PLAN**  
**for Implementation of the Information Security Management System**

|  |  |
| --- | --- |
| Code: |  |
| Version: |  |
| Date of version: |  |
| Created by: |  |
| Approved by: |  |
| Confidentiality level: |  |

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| YYYY-MM-DD | 0.1 | Dejan Kosutic | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc415647883)

[2. Reference documents 3](#_Toc415647884)

[3. ISMS implementation project 3](#_Toc415647885)

[3.1. Project objective 3](#_Toc415647886)

[3.2. Project results 3](#_Toc415647887)

[3.3. Deadlines 4](#_Toc415647888)

[3.4. Project organization 5](#_Toc415647889)

[3.4.1. Project sponsor 5](#_Toc415647890)

[3.4.2. Project manager 5](#_Toc415647891)

[3.4.3. Project team 5](#_Toc415647892)

[3.5. Main project risks 6](#_Toc415647893)

[3.6. Tools for project implementation, reporting 6](#_Toc415647894)

[4. Managing records kept on the basis of this document 6](#_Toc415647895)

[5. Validity and document management 6](#_Toc415647896)

# Purpose, scope and users

The purpose of the Project Plan is to clearly define the objective of the Information Security Management System (ISMS) implementation project, documents to be written, deadlines, and roles and responsibilities in the project.

The Project Plan is applied to all activities performed in the ISMS implementation project.

Users of this document are members of [top management] and members of the project team.

# Reference documents

* ISO/IEC 27001 standard
* ISO 22301 standard
* BS 25999-2 standard
* [decision or any similar document prescribing project launching]
* [methodology for project management]

# ISMS implementation project

## Project objective

To implement the Information Security Management System in accordance with the ISO 27001 standard by [date] at the latest.

## Project results

During the ISMS implementation project, the following documents (some of which contain appendices that are not expressly stated here) will be written:

* **Procedure for Document and Record Control** – procedure prescribing basic rules for writing, approving, distributing and updating documents and records
* **Procedure for Identification of Requirements** – procedure for identification of statutory, regulatory, contractual and other obligations
* **Scope of the Information Security Management System** – a document precisely defining assets, locations, technology, etc. which are part of the scope
* **Information Security Policy** – this is a key document used by management to control information security management
* **Risk Assessment and Risk Treatment Methodology** – describes the methodology for managing information risks
* **Risk Assessment Table** – the table is the result of assessment of asset values, threats and vulnerabilities
* **Risk Treatment Table** – a table in which appropriate security controls are selected for each unacceptable risk
* **Risk Assessment and Risk Treatment Report** – a document containing all key documents made in the process of risk assessment and risk treatment
* **Statement of Applicability** – a document which determines the objectives and applicability of each control according to Annex A of the ISO 27001 standard
* **Procedure for Internal Audit** – defines how auditors are selected, how audit programs are written, how audits are conducted and how audit results are reported
* **Procedure for Corrective Action** – describes the process of implementation for corrective and preventive actions
* **Form for Management Review Minutes** – a form used to create minutes from the management meeting held to review ISMS adequacy
* **Risk Treatment Plan** – an implementation document specifying controls to be implemented, who is responsible for implementation, deadlines and resources

Other documents which must be written during ISMS implementation are specified in the Risk Treatment Plan.

During the implementation of business continuity management the following documents (some of which contain appendices that are not expressly stated here) will be written:

* **Business Continuity Management Policy** – sets a basic framework for the BCMS, determines the scope and responsibilities
* **Business Impact Analysis (BIA) questionnaires** – analysis of qualitative and quantitative impacts on business, of necessary resources, etc.
* **Business Continuity Strategy** – defines critical activities, interdependencies, recovery time objectives, strategy for managing and ensuring business continuity, strategy for recovering resources, strategy for individual critical activities
* **Business Continuity Plan** – a detailed description of how to respond to disasters or other business disruptions, and how to recover all critical activities
* **Training and Awareness Plan** – a detailed overview of how employees will be trained to execute planned tasks, and how they will be made aware of the importance of business continuity
* **Business Continuity Exercising and Testing Plan** – describes how plans will be exercised and tested with the objective of identifying necessary corrective actions and improving the plan
* **BCMS Maintenance and Review Plan** – a detailed overview of how plans and other BCMS documents should be maintained to ensure their functioning in the case of business disruption
* **Post-incident Review Form** – a form used for reviewing effectiveness of plans after an incident

## Deadlines

Deadlines for acceptance of individual documents in the course of ISMS implementation are as follows:

|  |  |
| --- | --- |
| ***Document*** | ***Deadlines for document acceptance*** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Deadlines for acceptance of individual documents in the course of BCMS implementation are as follows:

|  |  |
| --- | --- |
| ***Document*** | ***Deadlines for document acceptance*** |
|  |  |
|  |  |
|  |  |
|  |  |

Final presentation of project results is planned for [date].

## Project organization

### Project sponsor

Each project has an assigned "sponsor" who does not actively participate in the project. The project sponsor must be regularly briefed by the project manager about the project status, and intervene if the project is halted.

[name, job title] has been appointed project sponsor.

### Project manager

The role of the project manager is to ensure resources necessary for project implementation, to coordinate the project, to inform the sponsor about the progress, and to carry out administrative work related to the project. Project manager's authority should be such as to ensure uninterrupted project implementation within set deadlines.

[name, job title] has been appointed project manager.

### Project team

The role of the project team is to assist in various aspects of project implementation, to perform tasks as specified in the project, and to make decisions about various issues that require a multidisciplinary approach. The project team meets each time before the final version of a document from section 2 of this Project Plan is completed, and in all other cases when the project manager deems it necessary.

*Table of participants in the project*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Name* | *Organizational unit* | *Job title* | *Phone* | *E-mail* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Main project risks

The main risks in the implementation of the project are the following:

1. Extension of deadlines in the risk assessment phase
2. Extension of deadlines during the development of business continuity plans
3. Performing activities that incur unnecessary costs and waste time
4. Selection of too many and/or too expensive controls

Measures to reduce the abovementioned risks are the following:

* The project manager monitors that all activities in the project are performed within defined deadlines, and seeks intervention by the project sponsor in a timely manner
* Hiring a consultant to ensure that time or resources are not spent on activities that are not important for the project, and that individual activities are not headed in the wrong direction
* Hiring a consultant to propose the most cost-effective controls

## Tools for project implementation, reporting

A shared folder including all documents produced during the project will be created on the local network. All members of the project team will have access to these documents. Only the project manager [and members of the project team] will be authorized to make changes and delete files.

The project manager will prepare a project implementation report on a monthly basis and forward it to the project sponsor.

# Managing records kept on the basis of this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Record name | Storage location | Person responsible for storage | Control for record protection | Retention time |
| Project implementation report (in electronic form) | Shared folder for project-related activities | Project manager | Only the project manager is authorized to edit data | The report is stored for a period of 3 years |

# Validity and document management

This document is valid as of [date].

Owner of this document is [job title].

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

* whether all employees engaged in the project perform their activities in line with this document
* whether all project deadlines are met

[job title]

[name]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[signature]