[organization logo]

[organization name]

**PROJECT PROPOSAL FOR ISO 27001/ISO 22301 IMPLEMENTATION**

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

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| xx/xx/2014 | 0.1 | Dejan Kosutic | Basic document template |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose 2](#_Toc384142166)

[2. Reasoning 2](#_Toc384142167)

[3. Project objectives 3](#_Toc384142168)

[4. Project duration and structure 3](#_Toc384142169)

[5. Responsibilities 3](#_Toc384142170)

[6. Resources 3](#_Toc384142171)

[7. Deliverables 4](#_Toc384142172)

# 

# Purpose

The purpose of this document is to propose the project of ISO 27001 and/or ISO 22301 implementation to the top management.

This document is not a project plan – the Project plan will be developed once the project is formally approved.

# Reasoning for the implementation

Primary reasons for ISO 27001/ISO 22301 implementation are:

* compliance with laws and regulations
* lower costs of incidents
* marketing advantage
* optimization of processes
* smaller dependence on individuals

# Project objectives

The objectives for the project are:

* implementation of ISO 27001 / ISO 22301 on or before [date]
* implementation of information security / business continuity may not interrupt normal operating activities
* members of the project team can spend up to [xyz%] of their time on this project

# Project duration and structure

The implementation project is divided into different phases:

1. Planning phase, including the development of top-level policy, risk assessment and risk treatment
2. Implementation of the selected controls
3. Internal audit
4. Management review
5. Certification

Main milestones of the implementation project are:

|  |  |
| --- | --- |
| **Milestone** | **Due date** |
| Planning phase |  |
| Implementation of the controls |  |
| Internal audit |  |
| Management review |  |
| Certification |  |

Detailed content of the milestones and respective responsibilities will be described in the Project Plan document.

# Responsibilities

Project will be led by [name], and project team members will be [list names].

# Resources

Resources required to implement the project include human, financial and technical resources.

Financial resources include:

* Amount: [define amount of money needed to finish the project]
  + Cost types: [split costs according to the cost type and include all resources listed here, e.g. human resources – internal and external, technical and other]

Human resources include:

* Internal resources – [list internal resources, e.g. group name, project name, etc.]
* External resources – [list all external resources, e.g. consulting company, etc.]

Technical resources include:

* Tool – tool name: [enter tool name]
* Equipment – [list equipment needed]

Other resources include:

* Documentation – [list all documentation that is required, e.g. ISO 27001 or ISO 22301 Documentation Toolkit, the standards, etc.]

# Deliverables

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. that 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 that 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 that must be written during ISMS implementation will be 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