CERTIKIT
Compliance made easy

ISMS Project Initiation Document

ISO/IEC 27001 Toolkit: Version 11

Implementation guidance

The header page and this section, up to and including Disclaimer, must be removed from the final version of the document. For more details on replacing the logo, yellow highlighted text and certain generic terms, see the *Completion Instructions* document.

Purpose of this document

This document defines what the project is to achieve and the resources allocated to its success.

Areas of the standard addressed

The following areas of the ISO/IEC 27001 standard are addressed by this document:

- 4 Context of the organization
  - 4.3 Determining the scope of the information security management system
- 5 Leadership
  - 5.1 Leadership and commitment
- 6 Planning

General guidance

A well written and agreed PID is essential to defining what the project is intended to achieve and clarifying what is in and out of scope. The PID may be one of the most important documents in your ISMS as it sets out the resources and timescales that will be used to establish the ISMS in the first instance.

Use the PID to gain consensus and commitment from management and staff to the implementation of the management system and the achievement of certification to the ISO/IEC 27001 standard.

Review frequency

The PID should be reviewed regularly throughout the project to ensure that the objectives set remain relevant and the expected business benefits will still be obtained.

Document fields

This document may contain fields which need to be updated with your own information, including a field for Organization Name that is linked to the custom document property "Organization Name".

To update this field (and any others that may exist in this document):

1. Update the custom document property "Organization Name" by clicking File > Info > Properties > Advanced Properties > Custom > Organization Name.
2. Press Ctrl A on the keyboard to select all text in the document (or use Select, Select All via the Editing header on the Home tab).
3. Press F9 on the keyboard to update all fields.
4. When prompted, choose the option to just update TOC page numbers.

If you wish to permanently convert the fields in this document to text, for instance, so that they are no longer updateable, you will need to click into each occurrence of the field and press Ctrl Shift F9.

If you would like to make all fields in the document visible, go to File > Options > Advanced > Show document content > Field shading and set this to "Always". This can be useful to check you have updated all fields correctly.

Further detail on the above procedure can be found in the toolkit *Completion Instructions*. This document also contains guidance on working with the toolkit documents with an Apple Mac, and in Google Docs/Sheets.

Copyright notice

Licence terms

Disclaimer

Please Note: Your use of and reliance on this document template is at your sole risk. Document templates are intended to be used as a starting point only from which you will create your own document and to which you will apply all reasonable quality checks before use.

Therefore, please note that it is your responsibility to ensure that the content of any document you create that is based on our templates is correct and appropriate for your needs and complies with relevant laws in your country.

You should take all reasonable and proper legal and other professional advice before using this document.

CertiKit makes no claims, promises, or guarantees about the accuracy, completeness or adequacy of our document templates; assumes no duty of care to any person with respect its document templates or their contents; and expressly excludes and disclaims liability for any cost, expense, loss or damage suffered or incurred in reliance on our document templates, or in expectation of our document templates meeting your needs, including (without limitation) as a result of misstatements, errors and omissions in their contents.

ISMS Project Initiation Document

DOCUMENT CLASSIFICATION	[Insert classification]
DOCUMENT REF	ISMS-DOC-00-1
VERSION	1
DATED	[Insert date]
DOCUMENT AUTHOR	[Insert name]
DOCUMENT OWNER	[Insert name/role]

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES

Distribution

NAME	TITLE

Approval

NAME	POSITION	SIGNATURE	DATE

Contents

Tables

1 Background

The International Standard for Information Security, ISO/IEC 27001, was announced by the ISO/IEC in 2005 and was updated in 2013. This was a development of the earlier British Standard, BS7799 and describes the actions necessary to establish an effective Information Security Management System (ISMS).

In [Date] a gap assessment was undertaken to assess the current level of conformity against the standard. This concluded that the organization is currently X% conformant and that "many required activities are carried out, but informally and are therefore not evidenced". Based on this report, [Organization Name] has decided to pursue full certification to ISO/IEC 27001 in order that the effective adoption of information security good practice may be validated by an external third party, a Registered Certification Body (RCB).

This document initiates the project to undertake the work that needs to be done within [Organization Name] to bring its information security processes and procedures in line with the standard and to achieve certification to it.

2 Objectives and benefits

2.1 Project objectives

The objectives of this ISMS Project are as follows:

1. To achieve certification to the International standard for information security, ISO/IEC 27001 within a X-month timeframe
2. To establish a more proactive information security framework within [Organization Name] in line with business requirements
3. To implement best practice in information security so that the organization's information assets are better protected
4. To increase the awareness of [Organization Name] staff of information security issues

Achievement of ISO/IEC 27001 certification will require [Organization Name] to invest time and money into the initial implementation project and the ongoing maintenance of the processes involved. It is important to be clear from the outset about the benefits that such a route is expected to deliver. As with many quality initiatives, it is difficult to put a monetary figure on the difference that certification will make (although sometimes this is possible if factors such as the cost of past information security breaches can be estimated).

2.2 Anticipated benefits

However, from the shared experience of previous implementations in other organizations of similar size it would be reasonable to anticipate the following major areas of benefit:

- Significantly reduced risk of harm, loss or embarrassment to the organization due to sensitive information loss
- Peace of mind assurance to our customers, staff, board members, suppliers and other interested parties that their data is secure
- Ability to bid for and respond to tenders for business where ISO/IEC 27001 certification is a requirement
- A public demonstration that [Organization Name] takes information security seriously
- Internal and external recognition of the quality of the information security controls in place
- Year-on-year improvement in the security of the organization's information assets as a result of the continuous improvement aspects of the standard
- A strong move away from reactive firefighting towards proactive security incident reduction
- Better alignment of information security controls with the needs of the business through regular review meetings with interested parties
- Better perception and awareness of information security issues within the business and IT user population as a whole

- Improved ability to manage information security breaches if they do occur, so reducing reputational damage and limiting business impact

Steps will be taken where possible to quantify the achievement of the project against these anticipated benefits.

3 Scope, dependencies, constraints and assumptions

3.1 Scope

[Define the areas that are *within* the scope of the project. This may be expressed in terms of geographical or organizational boundaries, products or services, systems, processes or any other factor that helps to define what is included.]

For the purposes of ISO/IEC 27001 certification, the boundaries of the certification are defined as follows:

"The management of information security in the provision of all products and services at all locations, within all business units of [Organization Name]"

The following areas will be explicitly defined as being out of scope:

[Define the areas that are outside the scope of the project. This may be expressed in terms of geographical or organizational boundaries, products or services, systems, processes or any other factor that helps to define what is excluded.]

3.2 Project dependencies

This project has the following inter-dependencies with other projects either planned or in progress within the organization:

PROJECT	NATURE OF DEPENDENCY	TIMESCALE
Data center relocation from Atlanta to Seattle	This project must be completed before ISO/IEC 27001 certification can be achieved	End of Q3 20xx

Table 1: Project dependencies

3.3 Constraints

The following constraints are applied to this project:

- The project must be achieved within the stated timescale
- Although limited financial resources are available, no specific budget has been allocated to this project, over and above the cost of the information security consultant

- The information security consultant is assigned to the project x days per week
- The project will be taking place at the same time as several other projects and so will need to compete for resources on a priority basis, decided by the [Finance Director]

3.4 Assumptions

In preparing this project initiation document, it is assumed that:

- Business managers are willing and available to participate in regular ISMS review meetings where appropriate
- Enough financial resources are available when required for any necessary expenditure recommended by the project
- Enough human resource is available to progress the project in a timely fashion

4 Project organization and authorities

It is important to define the way in which the project will be organized so that clear management direction will be possible.

4.1 Project organization

The project will be overseen by a project board which will have primary responsibility for the governance of the project and the achievement of its objectives.

4.1.1 Project board

The project board will consist of:

ROLE	NAME	TITLE
Project Sponsor	[Finance Director]	
Project Manager	[Information Security Manager]	
Senior Supplier	[Information Security Consultant] [Software tool Vendor]	
Senior User	[Business Manager]	

Table 2: Project board

The high-level project board roles, responsibilities and authorities are:

Project Sponsor

- Review and approval of project documentation
- Review and approval of processes defined by the project
- Approval of project change control
- Ad-hoc direction
- Approval of project closure

Project Manager

- Ensure the desired outcome of the project is specified and success criteria measured
- Manage the production of the required deliverables
- Plan and monitor the project

- Take responsibility for overall progress against plan
- Management of risks and issues
- Identification and management of project changes
- Project reporting and communication

Senior Supplier

- Attend project board meetings
- Represent the interests of the supplier organization
- Prioritize and allocate resources under their control

Senior User

- Attend project board meetings
- Represent the interests of the business operations areas involved
- Act as liaison between the project and business areas

4.1.2 Project team

The achievement of the project deliverables will be undertaken by the project team. The project team will consist of the following people:

ROLE	NAME	TITLE
Implementation lead		
Trainer		
Internal audit		
Project administration		
Technical lead		
Documentation writer		
Human resources		
Supplier management co-ordinator		
Legal adviser		

Table 3: Project team

The responsibilities of a Project Team Member are as follows:

- Input to one or more of the required deliverables
- Review of project documentation and deliverables
- Attendance at project meetings
- Input to risk and issue management
- Liaison with third parties within their area of responsibility

5 Project resources

The following resources will be allocated to the project by top management.

5.1 Human resources

The following people will be available to the project for the periods specified:

NAME	ROLE	PERIOD AVAILABLE	COMMITMENT
[Name]	Project Manager	6 months	5 days per week
[Name]	Technical lead	3 months	2 days per week

Table 4: Human resources

5.2 Technical resources

The following technical resources will be allocated to the project:

RESOURCE	PURPOSE	PROVIDED BY
Server capacity	Host new intrusion detection application	Service Delivery team
Network capacity	Connectivity for testing	Networks team

Table 5: Technical resources

5.3 Information resources

Information resources allocated to the project are as follows:

RESOURCE	PURPOSE	PROVIDED BY
Security Incident database	Analysis of risk areas	Help desk
Asset spreadsheet	Identification of information assets	Finance team

Table 6: Information resources

5.4 Financial resources

The following financial resources are available to the project.

RESOURCE	AMOUNT	AVAILIBILITY
Capital budget	USD 150,000	FY 20xx – FY20yy
Revenue Budget	USD 80,000 p.a.	Ongoing

Table 7: Financial resources

6 Timescales and milestones

The planned timescale of the project is to deliver the ISMS by [expected live date].

Within the overall timescale of the project it is envisaged that the following milestones will be achieved:

MILESTONE	TIMEFRAME
Gap Assessment	[specify date]
Project Initiation	[specify date]
Risk assessment completed	[specify date]
Management system in place	[specify date]
All required controls in place	[specify date]
First management review completed	[specify date]
Internal audit completed	[specify date]
Stage One Review	[specify date]
Stage Two Audit	[specify date]

Table 8: Milestones

Progress against these milestones will be tracked as part of project reporting and reviewed at project board meetings.

7 Project communication

7.1 Interested parties

Within the given scope of the project the following may be considered to be interested parties:

PARTY	NATURE OF INTEREST	COMMUNICATION METHOD
Project Board	Ensure project is successful	Weekly highlight reports
Organization staff	How change will affect current roles	Monthly updates via existing magazine
Business Managers	When new controls and procedures will be in force	Mailshot programme in run-up to go-live Attendance at management reviews
Suppliers	Compliance with control requirements	Email and regular meetings with key suppliers
Customers	Protection of customer data	Email and regular meetings with larger customers

Table 9: Interested parties

7.2 Project progress reporting

The project manager will produce a weekly highlight report for the project board, detailing progress last week, work scheduled for next week, issues outstanding, risk management actions and an estimate of the latest degree of conformance against the ISO/IEC 27001 standard.

7.3 RAID Log

The project manager will maintain a RAID log to record:

- Risks to the success of the project
- Actions agreed during project meetings
- Issues that are affecting the project
- Decisions made during the project

This log will be reviewed at each scheduled project meeting and upon significant changes affecting the project. The initial risks identified in this project initiation document will be used as a starting point.

8 Deliverables

The following major deliverables will be created as part of this project:

REF	DELIVERABLE	DESCRIPTION
1	ISO 27001 Gap Assessment	Assesses the current situation within [Organization Name] and what needs to be done to achieve ISO 27001
2	Set of information security policies	Defining the policy of the organization with respect to key aspects of information security
3	Statement of Applicability	Statement of which of the reference requirements of ISO27001 are applicable to [Organization Name]
4	Information Security Management System (ISMS) Policy	Documenting the way in which the ISMS operates
5	Other ISMS documentation	A variety of documents setting out how key aspects of the ISMS will function
6	Procedures and controls to address risk	An appropriate set of documentation to ensure that identified risks are addressed and treated satisfactorily
7	Risk Assessment and Treatment Process	How risk assessment and treatment is performed
8	Risk Assessment report(s)	Results of risk assessment using the defined process
9	Risk Treatment Plan(s)	What will be done about the identified risks
10	Information security records	Minutes of meetings, reviews, visitor books and other information security-related records
11	Training and awareness programs	Combination of formal training for key staff and briefings for all other staff
12	Audit reports	From internal and external audits
13	ISO/IEC 27001 Certificate	Evidence of certification to the ISO/IEC 27001 standard from a Registered Certification Body

Table 10: Deliverables

This list is in addition to deliverables produced as part of the management of the project e.g. project plans, progress reports.

9 Initial project risk assessment

At this stage in the project, the following potential risks have been identified:

RISK	IMPACT	LIKELIHOOD	SCORE	INITIAL TREATMENT
Loss of key staff	High	Low	**MEDIUM**	Involve staff in the project; encourage development via appropriate training
Lack of business buy-in to project	High	Low	**MEDIUM**	Involve business management; ensure regular and clear communication of project goals, benefits and progress
Insufficient resources	High	Medium	**HIGH**	Monitor progress against plan; raise issues to Project Sponsor if appropriate; delay project if required

Table 11: Project risk assessment

The treatment actions identified above will be taken by the project manager in order to address these risks.

10 Initial project plan

[Insert a copy of the initial project plan]