

**Information Security Context, Requirements and Scope**

ISO/IEC 27001 Toolkit Version 9

©CertiKit

|  |
| --- |
| **Implementation Guidance**  **(The header page and this section must be removed from final version of the document)** |
| **Purpose of this document**  This document sets out the organizational context of the ISMS. It describes what the organization does, how it does it, what factors influence the way it operates and the reasons for the definition of the scope of the ISMS. |
| **Areas of the standard addressed**  This document addresses many of the requirements in section 4 – “Context of the Organization” in the ISO/IEC 27001:2013 standard. This includes:  4. Context of the Organization  4.1 Understanding of the organization and its context  4.2 Understanding the needs and expectations of interested parties  4.3 Determining the scope of the ISMS  4.4 Information security management system |
| **General Guidance**  If your organization already has ISO9001 certification then much of the contents of this document may already be documented, in which case this information will need to be readily available at the ISO/IEC 27001 audit.  This is an absolutely key document that will need involvement from senior management to put together. In overview, it describes why an effective ISMS is needed and what may happen to the organization if one is not in place. The business impact analyses and risk assessments required by later sections of the standard will then define this in more detail.  As part of the implementation you may need to meet with the various interested parties to understand their view of the risk areas and consequences of failure. You may also need to obtain legal advice if your industry is subject to significant legal or regulatory requirements.  As with most of the documents in the ISMS you should ensure that all relevant parties are aware of the contents of this document, particularly as it sets out the need for additional procedures which may involve asking employees to do more work. Understanding the reason for this may reduce resistance to the ISMS within the organization.  It is worth spending some time getting the scope of the ISMS right as the other areas of the standard rely upon this. As with most international standards, it is acceptable to start with a limited scope definition and then to expand it over time as more familiarity and experience is gained by the organization. |
| **Review Frequency**  We would recommend that this document is reviewed as part of an annual exercise which should include significant business involvement to ensure that changed requirements are captured and feedback obtained. |
| **Toolkit Version Number**  ISO/IEC 27001 Toolkit Version 9 ©CertiKit. |
| **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) in Word 2010:   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 on the ribbon) 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 i.e. so that they are no longer updateable, then 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 then go to File > Options > Advanced > Show document content > Field shading and set this to “Always”. This can be useful to check that you have updated all fields correctly.  Further detail on the above procedure can be found in the *Toolkit Completion Instructions.* |
| **Copyright notice**  Except for any third party works included in this document, as identified in this document, this document has been authored by CertiKit, and is © copyright CertiKit except as stated below.  CertiKit is a company registered in England and Wales with company number 6432088. |
| **Licence terms**  This document is licensed on and subject to the standard licence terms of CertiKit, available on request, or by download from our website. All other rights are reserved. Unless you have purchased this product you only have an evaluation licence. If this product was purchased, a full licence is granted to the person identified as the licensee in the relevant purchase order. The standard licence terms include special terms relating to any third-party copyright included in this document. |
| **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.* |



**[Replace with your logo]**

**Information Security Context,**

**Requirements and Scope**

|  |  |
| --- | --- |
| **Document Classification:** | [Insert Classification] |
| **Document Ref.** | **ISMS-DOC-04-1** |
| **Version:** | **1** |
| **Dated:** | **[Insert date]** |
| **Document Author:** |  |
| **Document Owner:** |  |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Revision Author** | **Summary of Changes** |
|  |  |  |  |
|  |  |  |  |

**Distribution**

|  |  |
| --- | --- |
| **Name** | **Title** |
|  |  |
|  |  |
|  |  |

**Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Position** | **Signature** | **Date** |
|  |  |  |  |

**Contents**

1 Introduction 8

2 Organizational Context 9

2.1 Activities 9

2.2 Functions 9

2.3 Services 10

2.4 Products 10

2.5 Major Partnerships 11

2.6 Supply Chains 11

2.7 Objectives and Policies 11

2.7.1 Business Objectives 12

2.7.2 Business Policies 12

3 Internal and External Issues 13

3.1 Internal Issues 13

3.2 External Issues 13

3.3 Risk Appetite 14

4 Interested Parties and their Requirements 16

4.1 Interested Parties 16

4.2 Requirements 17

5 Purpose and Scope of the ISMS 19

5.1 Purpose 19

5.2 Potential Impact of an Information Security Incident 19

5.3 Information Security Objectives 19

5.4 Scope of the ISMS 20

5.4.1 Organizational 20

5.4.2 Products and Services 20

5.4.3 Activities 20

5.4.4 Exclusions 21

**List of Figures**

[*Figure 1 - Organization Chart* 10](#_Toc535846896)

**List of Tables**

*Table 1 - Requirements Summary of Interested Parties* 18

# Introduction

is committed to protecting the security of its business information in the face of incidents and unwanted events and has implemented an Information Security Management System (ISMS) that is compliant with ISO/IEC 27001:2013, the international standard for information security.

The purpose of this document is to describe the way the business operates, internal and external factors influencing it and to highlight in general terms the potential consequences of a security breach. This will allow the most appropriate mix of control measures to be put in place to reduce the level of risk and to ensure that plans are available and tested to manage the impact of any interruptions that do occur.

Specifically, this document sets out:

1. The context of the organization
2. External and internal issues relevant to the purpose of
3. Interested parties relevant to the ISMS
4. Information security requirements of these interested parties
5. The scope of the ISMS, including its boundaries and applicability

This document will be updated at least annually and when significant change happens to the relevant areas covered.

# Organizational Context

The organizational context of is set out in the following sections. Given the fast moving nature of the business and the markets in which it operates the context will change over time. This document will be reviewed on an annual basis and any significant changes incorporated. The ISMS will also be updated to cater for the implications of such changes.

## Activities

undertakes a wide range of business activities within its target sectors and is constantly developing new products and services to bring to market.

Describe:

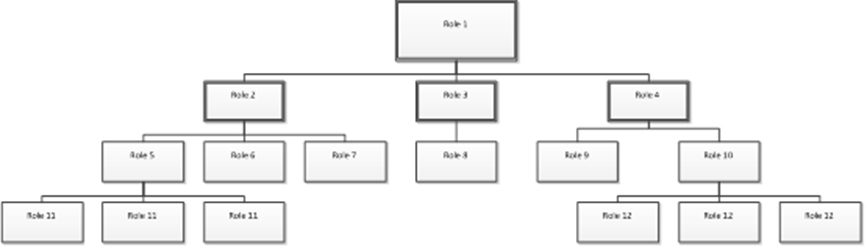
* What does the organization do?
* What type of cloud services are provided e.g. SaaS, PaaS, IaaS (CSPs only)
* When was it formed?
* What is its structure e.g. group of companies?
* What is its main industrial sector?
* Who are its main customers?
* In which geographical regions does it operate?
* What is its annual turnover?

## Functions

consists of the following organizational functions:

* Sales and Marketing
* Finance and Accounting
* Human Resources
* Operations
* Logistics
* Product Research and Development
* Project Management
* Risk and Compliance
* Consulting
* Information Technology
* Governance

An organization chart is shown below:



*Figure 1 - Organization Chart*

[Describe where the various functions are based e.g. HR, Finance and Marketing are in a corporate headquarters whilst Operations is in a regional structure spread across x offices nationwide/internationally. List where your data centres are located]

## Services

offers the following major services to its customers:

* [List the main cloud services provided if your organization is a CSP]

Specify:

* Are all services offered to all customers?
* Which services create the most revenue and profit?
* Are any services dependent on others (prerequisites)?
* Which services are the most high profile?
* Are any of the services subject to external regulation?
* Do any of the services have a health and safety aspect?
* To what extent is Personally Identifiable Information (PII) involved?

## Products

offers the following major products to its customers:

* [List the main products, if your company also provides products]

Specify:

* Are all products offered to all customers?
* Which products create the most revenue and profit?
* Are any products dependent on others (prerequisites)?
* Which products are the most high profile?
* Are any of the products subject to external regulation?
* Do any of the products have a health and safety aspect?

## Major Partnerships

has a policy of forming partnerships with other organizations which complement its own offerings and bring increased benefits to its customers.

The following major partnerships are currently in place:

For each partnership (if you have any) specify:

* Organization name
* Location(s)
* Nature of partnership
* Which products or services are affected by the partnership
* Which/how many customers are involved
* How long the partnership has been in place
* Is any PII shared with the partner
* Any other relevant information

## Supply Chains

In order to provide our products and services to our customers a number of important supply chain routes are in place. The major ones are:

Describe for each supply chain (if you have any):

* The products and services affected
* The links in the supply chain both in terms of organizations involved and geography
* How established the supply chain is
* Revenue and profit value that relies upon the supply chain
* Any other relevant information

## Objectives and Policies

The purpose of the ISMS is to ensure that is still able to meet its defined business objectives and comply with its policies in the face of potential and actual security incidents. This section sets out what the major business objectives and policies are for the current financial year so that a clear relationship can be established between these and the objectives of the ISMS.

### Business Objectives

For the financial year 20xx/20yy has set the following major business objectives:

* List the major business objectives – reference to business planning documentation may be made here

### Business Policies

Policies have been set by the organization in a variety of areas and these must be taken account of during the information security planning process to ensure that they are met. The main relevant policies are:

* Corporate Risk Management Strategy
* Human Resources Policy
* Home Working Policy
* Flexible Working Policy
* Equality and Diversity Policy
* Internet Acceptable Use Policy
* Information Security Policy
* IT Access Control Policy
* Legal Responsibilities Policy
* Other relevant policies

# Internal and External Issues

There are a number of internal and external issues that are relevant to the purpose of and that affect the ability of the ISMS to achieve its intended outcome(s).

## Internal Issues

With regard to the business itself, there are a number of relevant internal issues.

These include:

[List any specific internal issues e.g.

* Uncertainties in employee relations
* Significant organizational changes
* Location moves
* Company financial performance
* Company culture
* Resources and knowledge of the organization
* Governance and organizational structure
* Adopted standards and models
* Contractual relationships

You could choose to group internal issues using a SWOT analysis – Strengths, Weaknesses, Opportunities and Threats]

These general internal issues will be considered in more detail as part of the risk assessment process.

## External Issues

With regard to the external environment in which operates, there are a number of relevant external issues.

These include:

[List any specific external issues. These are often grouped under the areas defined by the term PESTLE e.g.

* Political
  + government policy changes
  + government instability
  + unrest in countries in which the organization operates
  + trade restrictions and tariffs
* Economic
  + prevailing economic climate
  + interest and inflation rates
  + supplier failure
  + lack of customer demand
  + increasing globalization of supply and/or demand
  + increasing competition
* Social
  + changing demographics
  + population growth changes
  + social attitudes
* Technology
  + pace of innovation
  + supporting technologies and infrastructure
  + automation and artificial intelligence
* Legal
  + potential legislative changes
  + regulatory changes
  + data protection
* Environmental
  + climate change
  + fire, flood, earthquake etc.
  + pollution]

These general external issues will be considered in more detail as part of the risk assessment process.

## Risk Appetite

The ISMS is designed to address the major risks that are identified to the information security of . In identifying, assessing and managing these risks there are a number of options open to the organization according to its appetite for risk.

In general terms the organization’s appetite for risk may be said to be Low/Moderate/High (delete as appropriate).

[Low] The strategy of the organization is to avoid risk where possible and to invest resources in mitigating residual risk through effective information security measures.

[Moderate] The strategy of the organization is to accept reasonable levels of risk whilst making some effort to ensure measures are in place to handle risks if they occur.

[High] The strategy of the organization is to accept significant levels of risk as an integral part of the business it is in, on the basis that the resulting rewards will be sufficient justification.

This general level of risk appetite will be applied to the risk assessments that are carried out as part of the ISMS and will determine the actions that need to be taken to mitigate risk to an acceptable degree.

The criteria for assessing risk in the context of the organization’s appetite for risk are defined in a separate ISMS document *Risk Assessment and Treatment Process*.

# Interested Parties and their Requirements

This section of the document sets out the interested parties that are relevant to the ISMS and their requirements. It also summarises the applicable legal and regulatory requirements to which the organization subscribes.

## Interested Parties

An interested party is defined as “a person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity”.

The following are defined as interested parties that are relevant to the ISMS:

* Shareholders
* Board of Directors
* Suppliers
* Customers
* Regulatory bodies
* Customer user groups
* Employees of the organization
* Contractors providing services to the organization
* National or local government organizations
* Emergency services
* Trade associations and industry bodies
* Trade unions
* General public
* Investors
* Distributors
* Competitors
* Media
* Neighbours
* Dependents of employees

If appropriate, list for each Interested Party:

* Name of organization
* The nature of the interest
* Degree of influence over the organization
* Value of the interest (if appropriate)
* Any other relevant information

Applicable legal and regulatory requirements arise from the following:

* Sarbanes-Oxley Act 2002 (USA)
* EU General Data Protection Regulation
* Health and Safety legislation
* Payment Card Industry – Data Security Standard compliance
* Financial Services legislation
* National and international standards e.g. ISO9001
* Consumer protection legislation
* [Specify laws and regulation relevant to your organization]

## Requirements

For details of how applicable legal, regulatory and contractual requirements are identified, accessed and assessed see the ISMS document *Legal, Regulatory and Contractual Requirements Procedure*.

The applicable requirements of interested parties and legal and regulatory bodies are summarised in the table on the following page.

|  |  |  |  |
| --- | --- | --- | --- |
| **Interested Party** | **Reqt.**  **Ref.** | **Requirement Summary** | **Source / link to supporting documents** |
| Shareholders | R1 | Value of share price should be maintained | Minutes of Annual General Meeting dd/mm/yyyy |
| Board of Directors | R2 | Value of share price should be maintained | Minutes of Board Meeting dd/mm/yyyy |
|  | R3 | Organisational reputation must be protected |
|  | R4 | Revenue stream must be maintained |
| Suppliers | R5 | Payment schedule must be kept to | Minutes of supplier meetings |
|  | R6 | Facility for receiving shipments must be available |
| Customers | R7 | Cloud service delivery should not be affected | Customer meetings/focus group sessions |
| Regulatory bodies |  | Etc. |  |
| Customer user groups |  |  |  |
| Employees of the organization |  |  |  |
| Contractors providing services to the organization |  |  |  |
| National or local government organisations |  |  |  |
| Emergency services |  |  |  |
| Trade associations and industry bodies |  |  |  |
| Trade unions |  |  |  |
| Sarbanes-Oxley Act 2002 (USA) |  |  |  |
| Health and Safety legislation |  |  |  |
| Payment Card Industry – Data Security Standard compliance |  |  |  |

*Table 1 - Requirements Summary of Interested Parties*

# Purpose and Scope of the ISMS

## Purpose

The purpose of the ISMS is to:

1. Understand the organization’s needs and the necessity for establishing information security management policy and objectives
2. Implement and operate controls and measures for managing the organisation’s overall capability to manage information security incidents
3. Monitor and review the performance and effectiveness of the ISMS
4. Continually improve the organization’s information security based on objective measurement

This purpose applies to the scope of the ISMS as defined below.

## Potential Impact of an Information Security Incident

The impact of any specific incident will obviously depend upon its nature and a comprehensive risk assessment is maintained to assess and mitigate those that can be reasonably identified. In general terms the potential impact of an inability to perform normal business processes will be shown in one or more of the following key areas:

* Loss of sales revenue
* Risk to life on health and safety grounds
* Loss of reputation/customer confidence
* Inability to meet our legal obligations
* Breach of contractual obligations
* Loss of business opportunity
* Fines and other penalties

[Explain which of the above apply to your organization and to what extent. Identify any other impacts that are specific to you].

## Information Security Objectives

Based on the requirements and issues set out in this document, the following major objectives are set for information security:

Define the main priorities that the ISMS must address, particularly in terms of the potential impacts described in section 3.3 of this document.

For example:

* Objective 1 - Comply with health and safety legislation at all times
* Objective 2 – Maintain shareholder confidence
* Objective 3 – Maintain customer service levels
* Objective 4 – Minimise loss of revenue
* Objective 5 - Avoid the loss of PII

The success of the ISMS will be judged on its ability to meet these overall objectives.

## Scope of the ISMS

The defined scope of ’s ISMS takes into account the internal and external factors referred to in sections 3.1 and 3.2 of this document and the requirements referred to in section 4. It also reflects the needs of interested parties and the legal and regulatory requirements that are applicable to the organization.

The scope is defined below in terms of the parts of the organization, products and services and related activities.

### Organizational

The ISMS includes the following parts of the organization:

[Specify the parts of the organization included in terms of business function, geographical location or other organizational boundary e.g. individual companies within a group structure]

### Products and Services

The following products and services are within the scope of the ISMS:

[List the products and services at an appropriate level of detail. This is more likely to be in the form of product and service types rather than specifics which are likely to change rapidly over time. The products and services selected must be consistent with the organizational split given in the previous section]

### Activities

The following activities are within the scope of the ISMS:

[List the business activities at an appropriate level of detail. The activities specified must be consistent with the organizational and product/service split given in the previous sections]

### Exclusions

The following areas are specifically excluded from the scope of the ISMS:

[Detail what is excluded and why, in terms of organizational parts, products / services and activities. This must remain consistent with the overall approach and not compromise the ability of the ISMS to produce the desired results and meet its objectives.]