|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Document Configuration** | | | | |
|  | |  | | |
| Document Title | | Information Security Context, Requirements and Scope | | |
| Document Subject | | XXXX’s ISO 27001 ISMS ‘scoping’ document | | |
| Document Number | | Version 1.0 | | |
| Document Issue Date | | ddmmyyyy | | |
| Author | | Information Security Officer | | |
| **Approval** | | | | |
| ***Name*** | ***Position*** | | ***Signature*** | ***Date*** |
|  |  | |  |  |
| **Version** **Control**   |  |  |  | | --- | --- | --- | | *Version* | *Date* | *Description* | |  |  |  | | This document contains XXXXX information and is the property of XXXX Limited. Distribution is restricted to XXXX Limited and restricted third parties as approved by the document owner. By accepting this document, the recipient agrees not to provide this document, or any information contained therein to any third party without express prior written consent of XXXX Limited. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without express or written permission of XXXX Limited. | | | | | | | |

Contents

[1 Introduction 3](#_Toc47353051)

[2 Organisational Context 4](#_Toc47353052)

[2.1 Activities 4](#_Toc47353053)

[2.2 Functions 4](#_Toc47353054)

[2.3 Services 6](#_Toc47353055)

[2.4 Major Partnerships 6](#_Toc47353056)

[2.5 Objectives & Policies 7](#_Toc47353057)

[2.5.1 Business Objectives 7](#_Toc47353058)

[2.5.2 Business Policies 7](#_Toc47353059)

[3 Internal & External Issues 9](#_Toc47353060)

[3.1 Internal Issues 9](#_Toc47353061)

[3.2 External Issues 9](#_Toc47353062)

[3.3 Risk Appetite 9](#_Toc47353063)

[4 Interested Parties and their Requirements 11](#_Toc47353064)

[4.1 Interested Parties 11](#_Toc47353065)

[4.2 Requirements 11](#_Toc47353066)

[5 Purpose and Scope of the ISMS 13](#_Toc47353067)

[5.1 Purpose 13](#_Toc47353068)

[5.2 Potential Impact of an Information Security Incident 13](#_Toc47353069)

[5.3 Information Security Objectives 13](#_Toc47353070)

[5.4 Scope of the ISMS 14](#_Toc47353071)

[5.4.1 Organizational 14](#_Toc47353072)

[5.4.2 Products and Service 14](#_Toc47353073)

[5.4.3 Activities 14](#_Toc47353074)

[5.4.4 Exclusions 15](#_Toc47353075)

# Introduction

XXXX. (XXXX) 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 XXXX;
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.

# Organisational Context

The organizational context of XXXX 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

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

XXXX was licensed in March 1990 and offers a range of specialist financial services to customers transacting with Africa including trade services, payments, treasury services, financing, advisory and wealth management.

XXXX is a limited liability company and a wholly owned subsidiary of XXXX. The company operates in the – (address)

The main industrial sector that the company operates in is Financial services.

The main customers of XXXX are Trade and Corporate entities dealing within sub-Saharan Africa.

## Functions

XXXX consists of the following organizational functions:

* Finance
* Operations
* IT
* Business Development
* Wealth Management
* HR
* Risk
* Audit

All functions listed above are based within the Head Office (address)

The data centres are located in ------

An organization chart is shown below:

Figure 1 - Organization Chart

The organisation chart can be found in the link below on the intranet

## Services

XXXX offers the following services to its customer base:

* Wealth management
* Trade services
* Payments services
* Treasury services
* Financing and advisory

## Major Partnerships

XXXX 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:

## Objectives & Policies

The purpose of the ISMS is to ensure that XXXX 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

XXXX has set the following major business objectives:

* Protection of revenue streams and company profitability;
* Ensuring the supply of goods and services to customers;
* Maintenance and enhancement of shareholder value;
* Compliance with legal and regulatory requirements

### 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:

* XXXX-POL-ALL-001 - Information Security Policy Framework
* XXXX-POL-ALL-002 - Acceptable Use Policy
* XXXX-POL-ALL-004 - Data Classification Policy
* XXXX-POL-ALL-008 - Business Continuity Management Policy
* XXXX-POL-ALL-009 - Access Control Policy
* XXXX-POL-ALL-010 - Remote Access Policy
* XXXX-POL-ALL-012 - Incident Response Policy
* XXXX-POL-ALL-013 - Disaster Recovery Policy
* XXXX-POL-ALL-014 - Vulnerability Management Policy
* XXXX-POL-ALL-015 - Security Awareness & Training Policy
* XXXX-POL-ALL-018 - Network Configuration Policy
* XXXX-POL-ALL-021 - Vendor Management & Due Diligence Policy
* XXXX-POL-ALL-022 - Telecommuting & Mobile Policy
* XXXX-POL-ALL-023 - Physical Security Policy

# Internal & External Issues

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

## Internal Issues

With regard to XXXX’s business itself, there are a number of relevant internal issues which include uncertainty in

* Employee relations.
* Significant organizational changes.
* Location movement
* Company financial performance.
* Company culture.
* Resources and knowledge of the organization.
* Governance and organizational structure.
* Adopted standards and models
* Contractual relationships.
* Human aspects such as competence of persons, organizational behaviour and culture.
* Operational factors such as process or production and service provision capabilities.
* Monitoring customer satisfaction.
* Factors in the governance of the organization, such as rules and procedures for decision making or organizational structure.

## External Issues

With regards to the external environment in which XXXX operates, there are a number of relevant external factors which include:

* Potential legislative or regulatory requirements.
* Social factors.
* Political factors and technological factors.
* Other factors considered shall include interfaces between XXXX and other third-party agencies providing services, regulatory function and other business inter-relation with XXXX.

## Risk Appetite

The ISMS is designed to address the major risks that are identified to the information security of XXXX. 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 Moderate.

* [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.

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
* Employees of the organization
* Contractors providing services to the organization
* National or local government organizations
* Emergency services
* Trade associations and industry bodies
* General public
* Investors
* Competitors

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. ISO27001
* Consumer protection legislation

## 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 are summarised in the Legal Regulatory and Contractual Requirements sheet link below.

# 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 and regulatory obligations
* Breach of contractual obligations
* Loss of business opportunity
* Fines and other penalties
* Inability to provide services to customers
* Loss of information assets

## Information Security Objectives

The objective of the XXXX Information Security is to protect the XXXX’s information assets from accidental or intentional loss, disclosure, attack or misuse. All reasonable measures shall be taken to ensure that:

* The XXXX’s information remains cXXXXX
* The integrity of information is maintained
* The XXXX’s requirements for the availability of information and the systems used to process information are met
* Accountability for information is maintained
* All appropriate regulatory and legislative requirements are met in full

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

## Scope of the ISMS

The defined scope of XXXX’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 XXXX organization:

Agreed scope location for the ISMS Implementation is **XXXX Limited (address)**. The following are the departments that are within scope of the ISMS:

* Finance
* Operations
* IT
* Business Development
* Wealth Management
* HR
* Risk
* Audit

### Products and Service

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

* Mortgages
* Loans
* Letters of Credit
* Bills Discounting
* Wealth Advisory
* Savings and Current Accounts
* Trade Financing

### Activities

The following activities are within the scope of the ISMS

* Wealth management
* Trade services
* Payments services
* Treasury services
* Financing and advisory

### Exclusions

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

The London office is excluded from the scope of the ISMS