|  |  |
| --- | --- |
| **Name** | Internal Audit Plan |
| **Version** | 1.0 |
| **Classification** | Internal |
| **Process Owner** |  |
| **Summary** | Document to perform Internal Audit for ISO 27001:2022, ISO 20000:2018 |
| **Approval** |  |
| **Date** |  |
| **Associated Records** | ISO 27001:2022, ISO 20000:2018 |

**HISTORY OF VERSION CHANGES**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Process Name** | **Key Change(s)** | **Version/**  **Revision** | **Dept** | **Date** | **Approval/Date** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**CHANGE INITIATION**

|  |  |  |
| --- | --- | --- |
| **Name** | **Department** | **Signature/Date** |
|  |  |  |

**TABLE OF CONTENT**

[1.0. INTRODUCTION 4](#_Toc517429062)

[1.1. Purpose 4](#_Toc517429063)

[1.2. Scope 4](#_Toc517429064)

[1.3. Objective 4](#_Toc517429065)

[1.4. Responsibilities 5](#_Toc517429066)

[2.0. INTERNAL AUDIT 5](#_Toc517429067)

[2.1. Audit period 5](#_Toc517429068)

[2.2. Audit criteria 5](#_Toc517429069)

[2.3. Audit methodology 5](#_Toc517429070)

[2.4. Appointment of internal auditor 6](#_Toc517429071)

[3.0. ANNUAL AUIDT PROGRAM 7](#_Toc517429072)

[3.1. Conducting internal audit program 7](#_Toc517429073)

[4.0. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 8](#_Toc517429074)

[5.0. INTERNAL AUDIT PROCEDURE 9](#_Toc517429075)

[6.0. NON-CONFORMITY AND CORRECTIVE ACTIONS 11](#_Toc517429076)

[6.1. Scope 11](#_Toc517429077)

[6.2. Responsibilities 11](#_Toc517429078)

[6.3. Procedure 12](#_Toc517429079)

[7.0. VALIDITY AND DOCUMENT MANAGEMENT 13](#_Toc517429080)

[8.0. SUPPORTING STANDARDS AND RELEVANT DOCUMENTS 14](#_Toc517429081)

# INTRODUCTION

This document specifies the internal audit plan for Information Security and Service Management Systems to be conducted by Information Systems Audit and Control Units in September 2019. The audit plan has been created following the guidelines for Information Security and Service Management Systems, auditing against the requirements of EN ISO 27001:2022 and ISO 20000:2018 as stipulated in EN ISO 19011:2018 (audit guideline).

This audit plan shall cover all relevant information for the audit, reflecting in particular planned on-site audit activities and requirements, allowing both the audit team and the auditee to prepare for the audit.

NOTE: This audit plan may be subject to changes after its release / distribution.

## Purpose

The purpose of the internal audit program is to contribute to the determination of the effectiveness of procedures, controls, processes, arrangements and other activities within the ISMS are in line with ISO 27001 and ISO 20000, applicable regulations, and the organization's internal documentation and confirm if they are maintained and meet policy requirements and set objectives.

# GENERAL INFORMATION

## Objective

The objective of the Internal Audit program is to;

contribute to the improvement of the ISMS & SMS and its performance

* fulfil the requirements for ISO27001 and ISO20000 certifications
* verify conformity with contractual requirements and
* determine the effectiveness of the ISMS & SMS
* the effectiveness shall be defined as the Group point average performance of the system not less than 80%, evaluated across all applicable control.

## Scope

The Internal Audit program applies to the Information Security Management System (ISMS) and Service Management System (SMS) in and its effectiveness to its Data Bank and IT operations as well as establish the requirements for planning, preparation, performance, reporting, follow-up and closedown of ISMS Internal Audit.

The audit criteria shall apply to two areas;

1. General requirements for Information Security and Service Management Systems, with focus on:
   * Top Management Commitment & Responsibility
   * Documentation
   * Scoping, Planning, Implementing, Monitoring/Reviewing and Continually Improving the Information Security and Service Management Systems
2. Process specific requirements and all applicable ISO27001 and IS020000 Annex controls (108) on a clause by clause evidence based approach.
3. The following controls were excluded and did not constitute part of the tested controls;

Exclusion to the ISMS Control

* A.18.1.5 Regulation of Cryptographic Controls.
* A.14.2.7 Outsourced development

## Internal Audit team

The following shall be audited;

* Top Management commitment
* Information Technology
* Information Security
* E-Business
* Business Process Re-engineering
* Loan Review
* Customer Service Management
* Brand and Marketing Communications
* Branch Operations Coordination
* Human Capital Management
* Corporate Banking
* Operational Risk
* Credit Risk Management
* Market Risk
* Remedial Asset Management
* Retail Products/Retail Operations
* Project Management
* Central Operations
* General Services
* Treasury
* Financial Control
* Management Information Systems
* Corporate Strategy and Planning
* Legal Services
* Compliance and Conduct
* Internal Audit
* Data & Innovation
* Sustainability and CSR
* Change Management

## Audit Schedule

The Audit shall be performed from 1st to 5th of July, 2019 between the hours of 9:00hrs to 17:00hrs daily;

# ANNUAL ACTIVITIES

This schedule may be subject to changes on short notice. See below a detailed schedule capturing the activities that shall constitute the audit.

Table 1: Internet audit Schedule

| Date | Time | Assessor | Business Area/Process | Role, Dept./Section |
| --- | --- | --- | --- | --- |
| Day 1  09/07/2019 | 08.30 | ISO 27001 LA  . | Opening Meeting and Tour of Facility | CISO, CIO, CRO, CAE, CCO, ISMS Manager, Service Delivery Manager, Project Manager and Change Manager |
| 09.00-10.00 | ISO 27001 LA | **Context of the Organization Clause 4**  Understanding the Organization and its Context Clause 4.1; Understanding the Needs and Expectations of Interested Parties Clause 4.2  Determining the Scope of the Information Security Management System (ISMS) Clause 4.3  Information Security; Management System (ISMS) Clause 4.4 | ISMS Manager/CISO/CIO/CAE/CRO/CCO |
| 10:00 – 10:30 | ISO 27001 LA | Leadership and Commitment Clause 5.1; Policy Clause 5.2; Organization Roles, Responsibilities and Authorities Clause 5.3 | ISMS Manager/ CAE/ CISO/ CIO/ CAE/ CRO/ CCO |
| 10.30 – 11.00 | ISO 27001 LA | Actions to Address Risks and Opportunities Clause 6.1; General Clause 6.1.1; Information Security Risk Assessment Clause 6.1.2  Information Security Risk Treatment Clause 6.1.3  Information Security Objectives and Planning to Achieve Them Clause 6.2 | Risk Management/Information Security |
| 11.00-12.00 | ISO 27001 LA | Resources Clause 7.1; Competence Clause 7.2  Awareness Clause 7.3; Communication Clause 7.4  Documented Information Clause 7.5: General Clause 7.5.1; Creating and Updating Clause 7.5.2  Control of Documented Information Clause 7.5.3 | HCM/BPR/Information Security/Brand and Marketing Communications/Customer Experience Management/ Sustainability and CSR |
| 12.00-12.30 | ISO 27001 LA | Operational Planning and Control Clause 8.1  Information Security Risk Assessment Clause 8.2  Information Security Risk Treatment Clause 8.3 | Risk Management/ Information Technology/ Information Security |
| 12.30-12.45 | ISO 27001 LA | Monitoring, Measurement, Analysis and Evaluation Clause 9.1; Internal Audit Clause 9.2  Management Review Clause 9.3 | Internal Audit/ Information Security |
| 12.45-1.00 | ISO 27001 LA | Non-conformity and Corrective Action Clause 10.1  Continual Improvement Clause 10.2 | Information Security/ Internal Audit |
| 1.00-2.00 | LUNCH BREAK | | |
| 2.00-3.00 | ISO 27001 LA | Review of Controls 5,6, | Information Security/Legal/Compliance and Conduct/ Project Management/ Treasury/ Central Operations/ Retail Operations/ Corporate Banking/ Branch Operations Coordination/ Corporate Strategy and Planning |
| 3.00-4.00 | ISO 27001 LA | Review of Controls 7,8,9 | Human Capital Management/Conduct and Compliance/Information Technology/ Information Security |
| 4.00-5.30 | ISO 27001 LA | Review of Controls 11,12 | Financial Control/ Management Information Systems/ General Services/ Information Technology/ Change Management/Information Security/ E-Business |
| DAY 2  10/07/2019 | 8.30-12.00 | ISO 27001 LA | Review of Controls 13,14,15 | Information Technology/ Project Management/Business Process Re-engineering/ Information Security/ Data & Innovation/General Services/ Internal Audit |
| 12.00-1.00 | ISO 27001 LA | Review of Controls 16, 17 | Information Technology/ Information Security |
| 1.00-2.00 | LUNCH BREAK | | |
| 2.00-3.00 | ISO 27001 LA | Review of Control 18 | Legal/ Compliance and Conduct/ Information Security |
| 3.00-4.30 | ISO 20000 LA | **4 Service management system general requirements**  4.1 Management responsibility  4.2 Governance of processes operated by other parties  4.3 Documentation management  4.4 Resource management  4.5 Establish and improve the SMS | SMS Manager/CIO |
| 4.30-5.30 | ISO 20000 LA | **5 Design and transition of new or changed services**  5.1 General  5.2 Plan new or changed services  5.3 Design and development of new or changed services  5.4 Transition of new or changed services | Information Technology |
| DAY 3  11/07/2019 | 9.00-1.00  2.00-4.30 | ISO 20000 LA | **6 Service delivery processes**  6.1 Service level management  6.2 Service reporting  6.3 Service continuity and availability management  6.4 Budgeting and accounting for services  6.5 Capacity management  6.6 Information security management  **7 Relationship processes**  7.1 Business relationship management  7.2 Supplier management | Information Technology/ Information Security/ Financial Control/ General Services |
| Day 4  12/07/2019 | 8.30-1.00 | ISO 20000 LA | **8 Resolution processes**  8.1 Incident and service request management | Information Technology |
| 1.00-2.00 | LUNCH BREAK | | |
| 2:00 – 5:30 | ISO 20000 LA | 8.2 Problem management | Information Technology |
| DAY 5  15/07/2019 | 8.30-12.30 | ISO 20000 LA | 9 Control processes  9.1 Configuration management  9.2 Change management  9.3 Release and deployment management | Information Technology |
| 12.30-3.30 | ISO 27001 LA  ISO 20000 LA | Report Writing |  |
| 3.30 – 4.30 | ISO 27001 LA  ISO 20000 LA | Report Presentation and Closing Meeting |  |
| 5.00 | ISO 27001 LA  ISO 20000 LA | End of Assessment | SMS Auditor |

NB: Conducted audits must be recorded in the Annual Internal Audit Program.

# **AUDIT METHODOLOGY**

## Audit approach

The audit shall utilize the evidence based approach as specified in the Internal Audit program, relying on the following evidence collection methods to audit the ISMS & SMS;

* Document Review
* Observation
* Interviews
* Analysis
* Technical verification

Note: In such instance where it is required to test the effectiveness of a control across a population, the random sampling technique shall be deployed. To determine the minimum sample required during the audit the sampling guideline as stipulated by IT Governance Institute shall be utilised (with a minimum of 4% to 6% margin of error) See table below.

Table 2: Sampling guideline

| Operational Mode of control to audit | Occurrence rate of operation | Minimum number of selection |
| --- | --- | --- |
| Manual | Several times a day  (Where population: > 366) | 25 |
| Manual | Daily  (Where population: 53-365) | 15 |
| Manual | Daily  (Where population: 13-52) | 5 |
| Manual | Daily  (Where population: 5-12) | 2 |
| Manual | Daily  (Where population: 1-4) | 1 |

## Expected Outcome

The internal audit can only lead to either of these 3 possible outcomes;

* Conformity: A conformity is said to have occurred when an organisation has fulfilled all requirements pertaining to a certain requirement
* Non-Conformity: A non-conformity is said to have occurred, when an organisation failed to fulfil a certain requirement. Four types of requirements exist (Requirements set in the ISO27001 & ISO20000 standards, Legislation on information security laws and regulations, Information security policies and procedure and requirements from 3rd party). Also, non-conformity can either be major or minor, a major Non-conformity means a total failure of the ISMS & SMS to meet a specific control objective.
* Observation: They are raised on activities that do not affect the ISMS & SMS, but can impact the ISMS & SMS on the long run and the auditors believe that there is an Opportunity for Improvement (OFI).

# VALIDITY AND DOCUMENT MANAGEMENT

This document is valid as of date of approval.

The owner of this document is the Internal auditor, who must check and, if necessary, update the document per individual ISMS & SMS audits.

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

* number of corrective actions identified in the previous audit
* number of corrective actions identified during the certification audit conducted after the internal audit
* whether the internal audit frequency is in line with the Annual Internal Audit Program