|  |  |
| --- | --- |
| **Name** | Internal Audit Program |
| **Version** | 2.0 |
| **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

XXXX Internal audit program specifies the objective, scope, duration and frequency of the Information Security Management System (ISMS) and Service Management System (SMS) audits. It establishes the requirements for initiating, planning, implementing audits of the ISMS & SMS and management of the internal audit program.

The audit program has been created under consideration to cover the post implementation period of the ISMS & SMS, prior to ISO 27001 & ISO 20000 certifications and after.

## 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 & SMS and ensure they are in line with ISO 27001 & ISO 20000, applicable regulations, and the organization's internal documentation and confirm if they are maintained and meet policy requirements and set objectives.

## Scope

The Internal Audit program applies to the Information Security Management System (ISMS) and Service Management System (SMS) at XXXX and its effectiveness to operations and establishes the requirements for planning, preparation, performance, reporting, follow-up and closedown of ISMS & SMS Internal Audit requirements.

## Objective

The objective of the Internal Audit program is to establish an independent system for verification of the implementation of the ISMS & SMS, and the improvement of it by means of a controlled method for planning, scheduling, coordinating and performing internal audits, and related activities.

Internal ISMS and SMS audits shall be conducted to provide information on whether the information security and Service management systems;

1. Conform to:

* the organization’s own requirements for its information security and Service management systems; and
* the requirements of the ISO 27001 & ISO 20000 Standards;

1. Are effectively implemented and maintained
2. Contribute to the improvement of the ISMS & SMS and their performance
3. Verify conformity with contractual requirements

## Responsibilities

The Chief Audit Executive is responsible for the overview and implementation of this program. Appointed Internal Auditors are responsible for the management and performance of the Internal Audit program in accordance with the requirements of ISO19011. All employees are responsible for assisting in the audit process, when required.

# INTERNAL AUDIT

## Audit period

The Internal Audit Program of the ISMS & SMS shall be done on an annual basis and shall cover the entire ISMS & SMS scope as specified in the ISMS & SMS scope documents as shown in table 1 below.

## Audit criteria

The Internal Audit criteria shall assume any of the following;

1. Audit against the requirements of ISO 27001 & ISO 20000.
2. Audit against documented policies and procedure.
3. Audit against 3rd party requirements like;

* Laws & Regulations
* Contractual agreement with Clients and vendors

## Audit methodology

The Internal Audit of the ISMS & SMS shall utilize the evidence based method and the following shall constitute the audit methodology;

* Observation
* Document review
* Interview
* Analysis
* Technical Verification

## Appointment of internal auditor

The Chief Audit Executive shall constitute audit team and appoint the internal auditors.

An internal auditor may be someone from the organization or a person outside the organization. Criteria for appointing internal auditors are:

* Knowledge of ISO/IEC 27001 and ISO 20000:2018 standards
* Familiarity with management system auditing techniques
* Knowledge of how information and communication technologies functions and the purpose of individual systems as well as the impacts on security processes

Internal auditors must be selected in such a way as to ensure objectivity and impartiality, i.e. to avoid conflict of interest as auditors are not allowed to audit their own work.

It is also recommended that internal auditors complete a course for internal auditors as specified in ISO/IEC 27001 and ISO 20000:2018.

# ANNUAL AUIDT PROGRAM

This annual program is written for the period from 10/09/2018 to 14/09/2018.

Internal audits according to ISO/IEC 27001 and ISO 20000:2018 standards will be conducted in the following way:

Table 1: Audit Program

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *Audit period* | *Audit scope* | *Audit criteria* | *Auditing method* | *Auditors* | *Status* |
| 01/06/2017 to  31/12/2017 | ISMS | * ISO27001 requirements * Documented policies and procedure * 3rd party requirements | * Document review * Process observation * Interviews | ISO 20000 LA  ISO 27001 LA |  |
| 01/01/2018 to  31/05/2018 | ISMS pre-surveillance audit. | * ISO27001 requirements (Continuous Improvement) * Documented policies and procedure * 3rd party requirements | * Document review * Process observation * Interviews | ISO 20000 LA  ISO 27001 LA |  |
| 10/09/2018 to 14/09/2018 | ISMS & SMS | * ISO27001 & ISO20000 requirements * Documented policies and procedure * 3rd party requirements | * Document review * Process observation * Interviews | ISO 20000 LA  ISO 27001 LA |  |
| 01/07/2019 to 05/07/2019 | ISMS & SMS  pre-surveillance audit. | * ISO27001 & ISO20000 requirements * Documented policies and procedure * 3rd party requirements | * Document review * Process observation * Interviews | ISO 20000 LA  ISO 27001 LA |  |

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

## Conducting internal audit program

Persons responsible for individual internal audits are identified in the Annual Internal Audit Program. If an audit is conducted by a team consisting of several auditors, the person responsible for the audit is the one identified as Audit Team Lead.

The following must be taken into consideration during an internal audit:

* criteria laid down in the Annual Internal Audit Program
* results of previous internal or external audits
* results of risk assessment, controls implementation and process gap assessment etc.
* Internal audit checklist

The following must be documented as internal audit results:

* Internal Audit Report must be sent to the Chief Audit Executive
* Possible corrective actions must be documented in the Corrective Action Form

# **MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT**

| Record name | Storage location | Person responsible for storage | Controls for record protection | Retention time |
| --- | --- | --- | --- | --- |
| Annual Internal Audit Program (in electronic form) | SharePoint Folder | Internal auditor | The Internal Auditor has right to make changes on this document, but not without authorization from the Chief Audit Executive. | Programs are stored for a period of 3 years |
| Internal Audit Report (in electronic form) | SharePoint Folder | Internal auditor | Reports are stored in read-only versions | Reports are stored for a period of 3 years |
| Internal Audit Checklist (filled form) | SharePoint Folder | Internal auditor | The checklist is stored in read-only version | The checklist is stored for a period of 3 years |

# INTERNAL AUDIT PROCEDURE

The Internal Auditor will plan and propose an ISMS & SMS audit schedules that will be reviewed and approved. The frequency of audit will depend on criteria such as;

* Business Need
* Severity of findings at most recent Internal Audit and internal ISMS & SMS compliance checks
* Programming of other audits in the same area
* Latest/proposed major revisions to processes, etc.
* Any other valid reason that may justly impact on the timing of an audit
* The Internal Auditor in conjunction with the ISMS Manager and SMS Manager shall establish the ISMS & SMS audit scope, as per the approved Audit Schedule
* Audit performance will be reviewed as part of the Management Review of the ISMS & SMS
* Audits will be conducted by an Internal Auditor who is trained to conduct that type of audit.
* Internal Auditors may undergo a variety of other types of audits to further develop their auditing skills. For specific types of audit, Internal Auditors will require special skills, (i.e. technical Audits for ISO27001 & ISO20000 compliance). Qualification requirements for these identified personnel are at the discretion of the Executive Leadership Team. Where there is no trained Internal Auditor, the solution may be through the appointment of a suitable third party.
* Human Resources maintains a record of training received by Internal Auditors and their suitability to conduct certain types of audit.
* During the planning and preparation for an audit, the Internal Auditors shall ensure that the following actions are taken:
* Preparation of an Audit Checklist
* Contact the Information Security and Information Technology teams to agree mutually convenient date(s) for the audit and to discuss the scope of the audits and audit criteria.
* The Internal Auditor conducts the audit using a checklist(s) as a guide. He/she examines the objective evidence and records relevant details. Internal Auditors may expand a checklist if additional questions become necessary, to determine the compliance with specified requirements and/or the effectiveness of a management system element.
* Confidentiality during audit: when an internal audit or third-party surveillance necessitates checking client files or databases, precautions must be taken to ensure that client confidentiality is preserved. Wherever possible, access is limited to satisfying the Internal Auditors that a file or database exists, is properly identified and is secure. If it is essential to check content, then access is limited to non-sensitive data.
* During an audit, the Internal Auditors shall evaluate the evidence found and analyze the apparent non-conformances to ensure their validity as audit findings. These findings must be communicated to the auditee as at time of observation.
* Where non-conformances are found and the corrective action agreed, the Internal Auditor will note the actions against the non-conformance. Where actions were completed at time of audit the Internal Auditors may sign off the non-conformance.
* Following completion of an audit, the Internal Auditors prepare a formal Audit Report comprising an Audit Lead Sheet, a number of Non-Conformities, one relating to each non-conformance identified (including those closed at the time of the audit), and additional sheets covering observations. The findings of the audit are summarized on the Audit Lead Sheet, including the number and nature of non-conformances.
* Where the Internal Auditor use supporting documentation, this may be inserted into the Audit Report as Observations, at the discretion of the Internal Auditor and in addition to the normal Audit Lead Sheet.
* The Internal Auditor obtains the signature of the lead audited entity (ISMS Manager & SMS Manager) on the Audit Lead Sheet, acknowledging the findings. A copy of the Audit Lead Sheet is given to the auditee for information and the complete report, together with all working papers, are sent to the Chief Audit Executive
* The Chief Audit Executive will document any working papers that do not form part of the official report separately.
* On receipt of the completed Audit Report, the ISMS & SMS Managers review the Observations, with a view to raising a Non-Conformance Report relating to each issue and then gives comments for each issue. Where the ISMS & SMS Managers have reasons to believe that the cause of the non-conformance may have resulted in similar non-conformances elsewhere, he/she may require follow-up audits to be carried out on that item, either in the originating area or other affected areas. These are planned in accordance with the process described above.
* Should follow-up audits prove necessary, they shall be undertaken in accordance with the requirements of this procedure.
* The results of audits shall be summarized and documented by the ISMS & SMS Managers in the ISMS & SMS Non-Conformities, Corrective and Preventive Actions (CAPA) Documents and reviewed at Management Review Meetings

# **NON-CONFORMITY AND CORRECTIVE ACTIONS**

## Scope

All problems and potential improvements identified within the Information Security and Service Management Systems fall within the scope of this procedure. This procedure also serves as an improvement suggestion scheme. The objective of this procedure is to ensure that problems, non-conformances, and improvements are dealt with in an efficient and effective manner, minimizing the chances of any recurrence. This procedure aims to ensure that processes, services and controls which do not conform to specified requirements are not used, or relied upon, until they are corrected. Complaints are subject to the same process described in this document.

## Responsibilities

Every individual involved directly or indirectly with XXXX Limited is responsible for initiating and complying with this procedure as and whenever it applies, and involves them.

The ISMS & SMS Managers are responsible for the overall control and operation of this procedure and for coordinating and processing all Non-Conformance issues in the ISMS & SMS Non-Conformities & CAPA (Corrective and Preventive Action) Documents.

Heads of Units are responsible for reporting non-conformities that are capable of resolution within their area to the Chief Audit Executive and the ISMS & SMS Managers.

## Procedure

* Findings (Observations and Non-conformities) from Internal Audit of the ISMS & SMS will be inputted in the ISMS & SMS Non-Conformities & CAPA documents by the respective Managers.
* Findings from Audits by an External Party will be inputted in the ISMS & SMS Non-Conformities & CAPA documents by the respective Managers.
* When a problem or potential improvement is identified, each staff has a duty to inform their unit managers of the issue, either verbally or by using a Non-Conformance Report.
* Any staff or third party, who becomes aware of an issue which does not meet XXXX’s defined approach and standards, or which has the potential for such an adverse effect, must raise a Non-Conformance Report immediately and forward it to the appropriate head of department.
* The ISMS & SMS Managers will evaluate the Head of Unit’s issue based on validity and priority. The issue will then be inputted in the ISMS & SMS Non-Conformities & CAPA documents by the ISMS & SMS Managers.
* The Head of Unit will agree a course of action and timescale to correct the issue, dependent upon the effect the issue is likely to have and to what degree. The agreed actions may rectify and prevent recurrence of the issue, or the consequences can be accepted. Such actions are recorded in the ISMS & SMS Non-Conformities & CAPA documents by the ISMS & SMS Managers.
* Timescales for completion should have regard to the cost/benefit of the non-conformance and other reasonable business priorities.
* The ISMS & SMS Managers will regularly monitor the progress of outstanding Non-conformities in the documents. If any action has not been completed by the previously agreed date, he/she will agree and record new actions and/or dates. If not satisfied that achievable progress is being made, they will escalate the matter to the higher line management responsible for that area.
* Non-Conformity & Observation issues will be closed down by the ISMS & SMS Managers once the issue has been addressed and proof of consideration to preventive measures can be demonstrated; this may result in a review by scheduled or additional Internal Audits. This will be recorded on the ISMS & SMS Non-Conformities & CAPA documents.
* During the Management Review of the ISMS & SMS (as stated in the ISMS Governance document), the ISMS Non-Conformities & CAPA document will be reviewed and Corrective Actions, Timelines, Due dates and effectiveness of the controls put in place, will be assessed by the Executive Leadership.
* The Executive Leadership team will take actions to control and correct these outstanding non-conformities and deal with the consequences. Issues and actions taken in these meetings will form updates for outputs of the Management review.
* The Executive Leadership Team shall also ensure that the organization;

1. evaluates the need for action to eliminate the causes of nonconformity (root cause analysis), and ensure that there is no reoccurrence elsewhere, by:

* Reviewing the nonconformity;
* Determining the causes of the nonconformity; and
* Determining if similar nonconformities exist, or could potentially occur;

1. implements any action needed;
2. reviews the effectiveness of any corrective action taken; and makes changes to the information security management system and/or Service management system, if necessary.
3. confirms that corrective actions are appropriate to the effects of the nonconformities encountered.
4. Learns from the records of actions taken and utilize the lessons for future improvement actions.

# 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 within the defined review cycle.

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

* number of corrective actions identified during the 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