[Company Name & Logo]

**Internal Audit Plan**

**Identifying and managing risks**

**Version: [v1.0]**

|  |  |
| --- | --- |
| Prepared by | |
| Name |  |
| Title |  |

[dd/mm/yyyy]

Table of Contents

[1. Introduction 3](#_Toc179825036)

[2. Objectives 3](#_Toc179825037)

[3. Scope 3](#_Toc179825038)

[4. Audit Schedule 4](#_Toc179825039)

[5. Roles and Responsibilities 4](#_Toc179825040)

[6. Audit Methodology 5](#_Toc179825041)

[7. Reporting and Follow-up 5](#_Toc179825042)

[8. Approval 6](#_Toc179825043)

## 1. Introduction

The purpose of this internal audit strategy is to ensure that the company complies with ISO 27001:2022 by outlining the goals, parameters, and timeline for internal audits. It is a crucial mechanism for evaluating the ISMS's efficacy and identifying areas in need of development.

## 2. Objectives

The key objectives of the internal audit program are:

* Evaluate the efficacy and the suitability of controls.
* Verify that the ISMS corresponds with ISO 27001 standards.
* Identify deviations and areas that need improvement.
* Confirm that the corrective steps have been implemented.

## 3. Scope

This internal audit program covers the following areas:

* ISMS Scope (as defined in the Scope and Context Definition document).
* Risk Management, Control Implementation, and Incident Management.
* Asset Management, Access Control, and Business Continuity Plans.
* All departments, processes, and systems involved in the ISMS implementation.

**Auditable Areas**:

* [Department 1]
* [Department 2]
* [Process/System 1]
* [Process/System 2]

## 4. Audit **Schedule**

The audit plan is set up in a way that guarantees that, during the scheduled audit cycle, all pertinent ISMS topics are addressed.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Audit No.** | **Area/Process** | **Audit Date** | **Auditor(s)** | **Notes** |
| 001 | Information Security Policy | [dd/mm/yyyy] | [Name/Team] | [Add any notes] |
| 002 | Asset Inventory and Control |  |  |  |
| 003 | Business Continuity Management |  |  |  |
| 004 | Risk Assessment Process |  |  |  |

## 5. Roles and Responsibilities

The following individuals and teams are responsible for executing the internal audit,

* **Audit Coordinator**: [Name/Role]  
  Responsible for overseeing the entire audit process, managing resources, and ensuring that audits are completed as scheduled.
* **Lead Auditor**: [Name/Role]  
  Responsible for leading individual audits, ensuring that all aspects of the area/process under review are assessed thoroughly.
* **Auditor(s)**: [Name/Role/Team]  
  Assist in conducting the audit by gathering evidence, interviewing staff, and identifying non-conformities.
* **Auditee(s)**: [Department/Name]  
  Provide relevant information, documentation, and access to systems for the audit process.

## 6. Audit Methodology

The internal audits will follow these steps:

1. **Planning**: Define the audit scope, objectives, and resources required.
2. **Execution**: Collect evidence through documentation review, interviews, and system walkthroughs.
3. **Reporting**: Summarize findings, including any non-conformities, observations, and areas for improvement.
4. **Follow-up**: Ensure that corrective actions are implemented and reviewed.

## 7. Reporting and Follow-up

Each audit will result in an **Internal Audit Report**, which will include:

* A summary of the audit findings.
* Identified non-conformities and observations.
* Recommendations for improvement.
* Deadlines for corrective actions.
* The responsible person or team for each action.

The **Audit Coordinator** will track the status of corrective actions and ensure follow-up audits are scheduled if necessary.

## 8. Approval

This Internal Audit Plan is reviewed and approved by:

* **Name**: [Audit Coordinator's Name]
* **Signature**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Date**: [dd/mm/yyyy]