Security Operating

Procedure

|  |  |
| --- | --- |
| **Procedure Name** | Internal Audit |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Version | Approved By | Owner | Date Last Updated | Review Frequency | Next Review | Comments |
|  |  |  |  |  |  |  |

**Classification**: Confidential

This document should be restricted to those with a specific need.

# Purpose of This Document

This document outlines the procedure for performing internal audits to ensure the Information Security Management System (ISMS) remains aligned with the ISO 27001 Information Security standard.

# Scope

The scope of this procedure is as follows;

* ISO 27001 and controls therein.
* The TechSolution.inc Information Security Management System (ISMS)

# Responsibilities

|  |  |  |
| --- | --- | --- |
| **Role** | **Responsibilities** | **Frequency** |
| Internal Auditor | * Conduct internal audit * Product report on findings * Present findings to ISG * Track progress over time | 6 monthly, minimum |
| Information Security Group (ISG) | * Review findings * Direct & track remediation activities for non-compliances | Upon audit results and monthly tracking of actions after that. |

# Procedure

## Overview

A diagram of a process

Description automatically generated

## Procedure Steps

**Step 1: Initiation**

* Every six months (minimum), the Internal Auditor will commence the audit.

**Step 2: Audit Plan**

* The Internal Auditor will document the scope of the audit, checking any changes in the ISO 27001 criteria and adjusting as necessary.
* The activities, timescales, and resources needed will be documented in the audit plan and emailed to the ISG to increase their awareness. If the ISG have any concerns about the audit's potential scope or business impact, they should advise the Auditor.

**Step 3: Interviews & Practices Review**

* Adhering to the Audit Plan, the Internal Auditor will review practices in alignment with the [Internal Audit Template](https://priassociation.sharepoint.com/:x:/s/InformationSecurity/ESzZ7A_pmwBHqXpY7d--tK0BK7X3a0nJUMxMZxcWpVAK3g?e=SGQFAX).
* The Auditor will review the results with the necessary managers/team leaders who implement the ISO 27001 guidance and, where necessary, front-line staff who carry out activities to ensure they are aware of procedures and policies.

**Step 4: Mandatory Documents & Records Evidence**

* The Auditor will collect examples of the ISO 27001 mandatory documents and records identified in the Audit Template above, linking evidence and examples in the audit results where possible.

**Step 5: Findings Report**

* The Auditor will complete the template, highlighting where the activities are in compliance and where they are not. The completed report should be distributed to the ISG for review. Textual commentary may be provided, if necessary, within the template.
* The Auditor will update the [Non-](https://priassociation.sharepoint.com/:l:/s/InformationSecurity/FOB1vHopTDRPtcHGNpuleRUBQmp3br8yftx64-FBRY4MxQ?e=9zybIg)Compliance Log with any findings that fall short of the ISO 27001 expectations. These findings may be categorised as follows;
  + **Non-Compliance** – Where the activities and evidence fall short of the ISMS expected standards
  + **Area of Improvement** – Where the criteria are broadly met, but improvements have been identified.
* Audit results will be filed in the [Audit Results](https://priassociation.sharepoint.com/sites/InformationSecurity/Audit%20Results/Forms/AllItems.aspx) repository.

**Step 6: Review the Findings**

* The Auditor will present the significant findings in person to the ISG, focusing on the non-compliances and gaps discovered in the report. The ISG may ask questions and choose to follow up where there may be disputes.
* The ISG will ensure that ownership is assigned to update the Risk Log for any identified risks that indicate vulnerabilities in the findings report.

**Step 7: Remediation Plan**

* The ISG will ensure that remediation actions are defined and added to [the Non-Compliance L](https://priassociation.sharepoint.com/:l:/s/InformationSecurity/FOB1vHopTDRPtcHGNpuleRUBQmp3br8yftx64-FBRY4MxQ?e=9zybIg)og items where the Auditor logged them during Step 5.