TrustIoT Framework for Industry 4.0

"Internal Audit Procedures"

|  |  |
| --- | --- |
| Document Classification: | Internal |
| Document Ref. | *TrustIoT Framework for Industry 4.0* |
| Version: | *1* |
| Document Author: | *Jibran Saleem* |
| Document Owner: |  |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Revision Author** | **Summary of Changes** |
|  |  |  |  |
|  |  |  |  |

**Distribution**

|  |  |
| --- | --- |
| **Name** | **Title** |
|  |  |
|  |  |
|  |  |

**Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Position** | **Signature** | **Date** |
|  |  |  |  |

Table of Contents

[1. Introduction 4](#_Toc190890155)

[2. Scope 4](#_Toc190890156)

[3. Roles and Responsibilities 4](#_Toc190890157)

[3.1. Information Security Management Representative (ISMR) 4](#_Toc190890158)

[3.2. Lead Auditor 4](#_Toc190890159)

[3.3. Audit Team Member 4](#_Toc190890160)

[3.4. Auditee 4](#_Toc190890161)

[4. Procedure 4](#_Toc190890162)

[4.1. General 4](#_Toc190890163)

[4.2. Planning and Preparing the Audit 5](#_Toc190890164)

[4.3. Pre-audit Meeting 5](#_Toc190890165)

[4.4. Opening Meeting 5](#_Toc190890166)

[4.5. Audit Execution 5](#_Toc190890167)

[4.6. Audit Reporting 5](#_Toc190890168)

[4.7. Closing Meeting 5](#_Toc190890169)

[5. Audit Follow-up and Closure 5](#_Toc190890170)

[6. Auditors Qualifications 6](#_Toc190890171)

[6.1. Personal attributes 6](#_Toc190890172)

[6.2. General knowledge and skills: 6](#_Toc190890173)

[6.3. Lead Auditors' Qualifications: 6](#_Toc190890174)

[6.4. Specific Knowledge and Skills of IoT Auditors: 6](#_Toc190890175)

[7. Document Management 6](#_Toc190890176)

# Introduction

To ensure that Companie’s IoT ecosystem operates in alignment with security policies, procedures, and industry best practices, and to identify opportunities for enhancing the security posture of IoT devices and related processes.

# Scope

This procedure encompasses the planning, execution, reporting, and follow-up of audits focused on IoT devices and their integration within Company’s environment. It applies to all departments and business units utilising IoT devices.

# Roles and Responsibilities

## Information Security Management Representative (ISMR)

* Appoints the Lead Auditor and the Audit Team.
* Reviews corrective and preventive actions and follow-up audits based on the internal audit report.
* Maintains confidentiality of audit results.

## Lead Auditor

* Prepares an Audit Plan/Notification.
* Leads IoT audit activities.
* Coordinates the audit schedule.
* Plans the audit, prepares working documents, and briefs the audit team.
* Consolidates audit findings and prepares the internal audit report.
* Reports critical non-conformities to the auditee immediately.
* Conducts opening and closing meetings.

## Audit Team Member

* Supports the Lead Auditor.
* Performs the audit using the provided checklists.
* Reports non-conformities and recommends improvements.
* Maintains confidentiality of audit findings.
* Acts ethically at all times.

## Auditee

* Receives, considers, and discusses the audit report.
* Determines, resources, drives, and completes corrective actions.
* Remains accountable for IoT device security.

# Procedure

## General

* An IoT audit program shall be created annually, encompassing scheduled and potential audits.
* Internal IoT audits shall be scheduled at least annually or as needed.
* Only competent and independent personnel shall perform audits.
* The Audit Team shall be appointed by the ISMR.
* An Audit Notification Memo shall be sent at least three working days in advance.

## Planning and Preparing the Audit

* The Lead Auditor shall prepare an annual IoT audit program, approved by the IT Department.
* The Lead Auditor shall prepare audit plans based on the program.
* The Audit Plan/Notification shall be prepared by the Lead Auditor, reviewed and approved by the ISMR, and communicated to all parties.
* The plan shall include audit objectives, scope, departments/individuals responsible, audit team members, IoT systems to be audited, date/time/location, and report distribution date.

## Pre-audit Meeting

* A pre-audit meeting shall occur between the ISMR, Lead Auditor, and auditors to ensure resource availability, verify the audit scope, and address logistical matters.

## Opening Meeting

* An opening meeting may be held to discuss the audit's purpose, scope, confirm the plan, and clarify any matters.

## Audit Execution

* Auditors shall utilise checklists, including:
  + IoT Device Security Checklist
  + Network Connectivity and Security Checklist
  + Data Protection and Privacy Checklist
  + IoT-Specific Risk Assessment Checklist
* Audit findings shall be collected through interviews, document examination, and observation.
* Evidence of non-conformities shall be noted, even if not on the checklist.

## Audit Reporting

* Auditors shall have a wash-up meeting to review findings, consolidate and classify them, and prepare recommendations and the audit report.
* Findings shall be classified as major non-conformity, minor non-conformity, improvement potential, or positive findings.
* The Lead Auditor shall prepare a standard internal audit report containing audit details, findings, references to standards, corrective/preventive actions, follow-up actions, and verification.
* Auditors shall adhere to a code of conduct for reporting, ensuring conciseness, factual accuracy, constructiveness, objectivity, and scope adherence.
* The Lead Auditor shall issue a formal Audit Report to the ISMR.
* The report shall be maintained and controlled by the ISMR.

## Closing Meeting

* The Lead Auditor shall preside over the closing meeting, where findings, observations, and recommendations are presented.
* Confidentiality of the report shall be maintained.

# Audit Follow-up and Closure

* Auditees are responsible for resolving non-conformities within agreed-upon timeframes.
* The Lead Auditor shall follow up to verify corrective action implementation.
* An audit is closed only when all corrective actions are successfully implemented.

# Auditors Qualifications

## Personal attributes

* Auditors shall possess ethical conduct, open-mindedness, diplomacy, observation skills, perceptiveness, versatility, tenacity, decisiveness, and self-reliance.

## General knowledge and skills:

* Audit principles, procedures, and techniques
* Management system and reference documents
* Organisation/business context
* Applicable laws and regulations

## Lead Auditors' Qualifications:

* Additional skills in audit leadership, planning, resource management, team motivation, conflict resolution, and report preparation.

## Specific Knowledge and Skills of IoT Auditors:

* IoT security terminology and concepts
* IoT security management principles and tools
* IoT-specific processes, technologies, and risks

# Document Management

This document is valid as of [dd/mm/yyyy].

This document is reviewed periodically and at least annually to ensure compliance with the following prescribed criteria.

* Compliant with the Internet of Things (IoT) Security Framework for Industry 4.0.
* Legislative requirements defined by law, where appropriate.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Name 1]

Manager