Internal Audit Procedure

KG Invicta Services (KGiS)

[Ref: ISM-PLC-DOC-03]
[Ver: 1.0]
[05th April 2023]
[Classification: Internal]

+91 422 4419999

KGiS
o 365, KG Invicta Services Private Limited KGiSL Campus, Thudiyalur Road, Saravanampatti, Coimbatore - 641035, India

www.kginvicta.com

Statement of Confidentiality

This document contains confidential and proprietary information of KG Invicta Services Private Limited (KGiS). It is furnished for KGiS internal use and purpose only. Except with a prior written permission of KGiS, this document and the information contained herein may not be published, disclosed, or used for any other purpose. This document is reviewed at least annually.

Copyright and Intellectual Property

a. KGiS logo are registered marks of KG Invicta Services Private Limited.

b.

Table of Contents

1 Document Control

1.1 Document Owner and Approval

KGiS's Information Security Office (ISO) is the accountable owner of this procedure. The ISO is responsible for ensuring that this document is reviewed periodically by the relevant stakeholders in line with the review requirements of the Information Security Management System (ISMS).

A current version of this document is available to all KGiS members at the corporate Intranet and is published on 05th April 2023.

This procedure document was approved by the Head of ICT on 05th April 2023 and met the required Documentation Quality Standard and is issued on a version-controlled basis under the signature.

Name: Shanmugam C

Designation: GM - ICT

Signature: Date: 05th May 2023

1.2 Amendment History Record

Version	Description of Change / Action	Resource	Date
1.a	New draft baseline of ISMS procedure	Harikrishnan P	04th May 2023
1.0	Verified and Approved By	Shanmugam Chinnasamy	05th May 2023

1.3 Cross References

All reference documents available in – Shared Folder
ISO 27001– Information technology – Security Techniques – Information security – Requirements
ISO 27002 – Information technology – Security techniques – Code of practice

1.4 Document Sign off and Distribution

Name	Designation	Signature	Version	Date
Shanmugam Chinnasamy	GM- ICT		1.0	05th May 2023

Document Distributed for Internal Approval.

Stakeholder	Date
All Head of Departments and Departments	

2 Definitions & Glossary

Term	Definition
ISO / IEC	International Organization for Standardization / International Electro technical Commission.
Root Cause Analysis	Root cause analysis is a set of problem-solving methods aimed at identifying the root causes of an incident/event. Root cause analysis results in elimination of the root causes instead of solving it to contain the current situation.
Preventive Action	A preventive action is a planned control implemented to eliminate the cause of potential non-conformities, that may be foresighted during a management review, risk assessment, performance measurement etc in order to prevent their occurrence.
Corrective Action	A corrective action is a planned control implemented to eliminate the cause of non-conformities that may rise due to violation of any management system controls, requirements, customer complaints, incidents or weaknesses etc. in order to prevent their recurrence.
Confidentiality	To ensure that data/ information is not made available or disclosed to unauthorized individuals, entities
Integrity	To ensure accuracy and completeness of the data/ information is maintained. Modifications to the information is made only by authorized individuals
Availability	To ensure that data/ information is made available, accessible, and usable for authorized personnel.
Auditee	Auditee is a person who gets audited by the auditors during the Internal audit process.
Non-Conformance	Non-Conformances (NC's) are the points where the organizational controls fail to comply with the information security policies and procedures.

3 About the Document

3.1 Introduction

The Internal audit procedure plays a vital role in assessing the effectiveness and compliance of an organization's internal controls, processes, and systems. It is a systematic and independent examination of operations carried out by qualified internal auditors within the organization. The purpose of internal auditing is to provide objective and unbiased evaluations that contribute to improving risk management, governance, and overall organizational performance.

This introduction aims to provide an overview of the Internal Audit Procedure and its significance in promoting transparency, accountability, and continuous improvement within an organization. It outlines the key objectives, scope, and benefits of conducting internal audits, highlighting their role in identifying weaknesses, mitigating risks, and enhancing the efficiency and effectiveness of internal operations.

3.2 Objective

The objective of this procedure is to provide assurance to management and stakeholders that the organization's operations are conducted in accordance with established standards, controls, and best practices. It helps the organization identify areas of improvement, mitigate risks, and maintain a strong governance framework for sustainable growth and success.

3.3 Scope

This procedure applies to all information assets management owned or managed by the KGiS ICT staff (permanent, contract employees, and students), and external parties (contractors, consultants, vendors, suppliers, partners and customers)

3.4 Roles and Responsibilities

- The Head of ICT is responsible to:
  - Review and approve the procedure to ensure that it reflects the current requirements.
  - Confirm the appointment of internal Auditors for conducting internal audits.
  - Provide required support during implementation of corrective and preventive controls.
  - Provide guidance for successful closure of all reported non-conformities.
- The Information Security Steering Committee (ISSC) is responsible to:
  - Review and approve the audit findings.
  - Provide required support during implementation of corrective and preventive controls.
- The Information security Officer (ISO) is responsible to:
  - To ensure adherence to this procedure.
  - Reviewing and updating this procedure to meet KGiS requirements.
  - Support respective process owners in conducting root cause analysis for reported non-conformances.

- Ensure corrective and preventive actions are identified as per the corrective and preventive action procedure.

- The Internal auditor is responsible to:
  - Plan, conduct and manage the internal audit process.
  - Present audit plan to the steering committee for approval.
  - Capture necessary evidences during the audit.
  - Create non-conformance reports.
  - Proving clarifications on queries related to audit findings.
  - Present audit findings to the steering committee for approval.
  - Prepare consolidated and individual audit reports.
  - Finalize implementation dates on audit findings in coordination with ISO and process owners.
  - Track implementation of planned controls
  - Verify timely closure of the non-conformances during subsequent audit cycle.
- Auditee is responsible to
  - Act as point of contact for audits in their respective processes
  - Support auditors during audits of their respective processes
  - Provide necessary evidence to demonstrate compliance with the policies and procedures.
  - Ensure necessary people are available during the audit process.

4 Procedure

The processes that need to be followed for the effective implementation and management of this procedure are explained in this section.

The internal audit procedure includes the following main stages:

- Planning
- Pre-audit Preparation
- Execution
- Reporting
- Tracking & Closure

4.1 Planning

- Information Security Management System (ISMS) internal audit should be conducted by the Internal auditor on a quarterly basis.
- The annual internal audit plan should be decided at the start of each year by the Internal Auditor and communicated to the Information Security Steering Committee.
- The annual internal audit plan should include the following details:
    - Expected start and end date of an internal audit.
    - Expected scope of audit- processes/functions.
    - The Internal auditor should create a detailed Internal Audit Plan at least one month prior to the scheduled internal audit.
- The detailed internal audit plan should include the following details:
    - Exact start and end date of the internal audit.
    - Exact scope of the audit – process/functions.
    - Locations to be covered during the audit.
    - Date and time of audit for each process/function.
    - Type of audit - Process or Technical.
- The internal auditor can include external parties to support the internal audit. In such cases, the Internal auditor should supervise and coordinate with the external party while conducting the audit.
- Once the detailed internal audit plan is ready, the Internal Auditor should have the detailed plan approved from the Information Security Steering Committee.

4.2 Pre-Audit Preparation

- On approval, the internal auditor should communicate the detailed internal audit plan to all concerned auditees.
- The internal auditor should ensure that the ISMS internal audit checklist is updated as per the current information security policies and procedures of KGiS.
- The internal auditor on the first day should initiate the audit with an opening meeting with all the auditees of the concerned processes/functions that fall under the scope of the internal audit. The internal audit opening meeting should be used to:
    - Set the objectives of the audit.
    - Discuss the scope of the audit.
    - Reconfirm the date and time for auditing individual processes.
    - Communicate the expected support including availability of the people from the auditees.
    - Communicate the planned date and time for the closing meeting.

4.3 Execution

- The internal auditor is responsible for overall coordination and conducting of the internal audit.
- The internal auditor should ensure the internal audit is conducted as per detailed internal audit plan with the changes discussed during the opening meeting.
- The internal auditor can use the ISMS internal audit checklist as reference to ensure all relevant controls of ISO 27001 standard are covered.
- The internal auditor as part of the internal audit can also verify compliance to other relevant organization policies/procedures and industry best practices.
- The internal auditor should conduct a sample audit to measure the effectiveness of the implemented information security controls. The auditor at his/her discretion can also take a larger sample or do a comprehensive audit of the process/facility.
- The ISMS internal audit should be conducted through any or all of the following key steps:
    - Through interviews process/function owners.
    - Review documents and records as deemed necessary.
    - Review of technical configurations of equipment's as deemed necessary.
    - Using technical tools which have been approved by the Information Security Steering Committee.
    - Offline audit by collecting all evidences from relevant stake holders.
- The internal auditor should check the following during the internal audits:
    - General awareness among employees about the current information security practices.
    - Implementation of information security controls in the process/function.

    - Effectiveness of implementation of an information security control.
    - Necessary evidence of implementation of an information security control.
    - Ability of the current information security practices to address any new risks.
    - Additional information security controls that can improve the overall security posture of the organization.
- The internal auditor at the end of the audit with a specific process/function team should summarize the observations/findings with the respective process/function owner.
- The internal auditor should ensure that the observations and findings (non-conformances) captured during the audit are recorded properly for future references.
- The internal auditor wherever deemed necessary and feasible, should capture evidence of non-conformities observed during the audit.
- The internal auditor should ensure that evidence captured during an audit are shared on a need basis and only after proper authorization from the Head of ICT.
- The internal auditor should ensure that details of non-conformities captured during an audit are not disclosed with any external party without prior authorization from the Head of ICT.
- The internal auditor on completion of the internal audit should conduct an internal auditor closing meeting with all the auditees for the following:
    - Present strengths observed during the audit.
    - Present weaknesses (non-conformances) observed, if any.
    - Clarify on any observations.
    - Respond to any queries on information security.
    - Finalize tentative date for release of the internal audit report.

4.4 Reporting

- The internal auditor, on completion of the defined scope of audit, should compile the non-conformances in an internal audit report.

Types of Non-Conformances

- All kinds of non-conformances of an internal audit should be categorized into any one of the following as mentioned below:

Type of non-conformances	Probable Reasons for the Non-Conformance
Major Non-Conformance	A Major non-conformance may occur due to any of the following reasons:

	1. When one of the ISO 27001 control or control objective has not been addressed adequately even though it is applicable as per the Statement of Applicability (SOA). 2. Most of the requirements of a particular policy, procedure and standard are not addressed. 3. Information security policy or procedure is defined but not yet adopted or implemented by the concerned departments. 4. If a current information security practice has a serious gap which can lead to compromise of information assets. 5. If a significant number of minor non-conformances in a given area point to a systemic failure. For example, a minor nonconformance in document control may not in itself constitute a significant problem. But if several non-conformances are found with document control, then this may point to a larger problem in document control and would constitute a major nonconformance.
Minor Non-Conformance	A minor non-conformance may occur due to any of the following reasons: 1. A non-conformance that doesn't indicate to a bigger problem in the ISMS and can be construed as an isolated or random incident. 2. If a current information security practice has very minimum gaps that cannot be exploited by a threat or even if exploited may result in low value risk. 3. Some examples of a minor non-conformance are: • The asset register is not getting updated with the latest modifications or additions of assets. • The most current version of a document is not available at an operator's station; the updated version exists but a copy of it is currently not available with the operator.
Observation	An observation may occur due to any of the following reasons: 1. No direct violation to the policies, procedures and standards but an identification that there may be a better way of performing an activity. 2. Observations for improvement to avoid future problems. 3. A suggestion so that a non-conformance is not created in future.

- The internal audit report should be prepared as per the standard report template.

4.5 Tracking and Closure

- The respective process/function owners with support from the Head of IT should ensure that the reported non-conformities are closed prior to the implementation dates as mentioned in the Non-Conformance response form of the Internal Audit Report.
- The Information Security Office should proactively support the Information Security Champion to ensure closure of the non-conformities on a timely basis.
- The Internal Auditor should track the closure of the non-conformances with the respective process/function owners on a proactive basis and request them to submit a status report on the NC closure status.

4.6 Roles and Responsibilities Matrix

Roles/ Responsibilities	Internal Auditor	Auditee	ISSC
Planning	R	C	A, I
Pre-audit Preparation	R	C	A, I
Execution	R	A,C	I
Reporting	R	A,C	I
Tracking & Closure	R	A,C	I

R Responsibility – The personnel who is responsible for performing the task.

A Accountability – The personnel who is accountable for the process or data.

C Consulted – The personnel who provide opinions or suggestions.

I Informed – The personnel who should be informed with the progress and updates.

5 Record Template

Following are the records that get developed as a part of this process – Internal Audit Procedure

- Internal Audit Schedule

Schedule.docx

- Non-Conformance Form

NC%20forms.docx

- Non-Conformance Tracker

Non-Conformance Tracking .xlsx