ISO 27001 Internal Audit Report for KG Invicta Services Private Limited (KGiS)

Report Name:	ISO 27001 Internal Audit Report for KGiS
Version Detail:	1.0
Report Owner:	Green IT
Report Classification:	Confidential
Report Status:	Final
Report Date:	12.06.2023

REPORT REVIEW & APPROVALS

The signatures below certify that this procedure has been reviewed and accepted and demonstrate that the signatories are aware of all the requirements contained herein and are committed to ensuring their provision.

SIGN OFF				
Responsibility	**Date**	**Name**	**Designation**	**Signature**
PREPARED BY	12 June 2023	Green IT – Manoj Durai	Lead Auditor –ISMS	
REVIEWED BY	13 June 2013	Green IT – Durai Raj Manickam	Technical Lead	

We have completed our review of ISO/IEC 27001:2013 we are pleased to submit our report herewith. The purpose of this internal audit review was to evaluate the design, operational effectiveness and adequacy of the controls related to ISO 27001:2013 standard requirements. The report contains the exceptions identified to 27001 standard and has the findings and recommendations. We would like to draw your attention to the observations highlighted in the executive summary where significant opportunities for improvement have been mentioned.

Contents

1. Assessment Objective, Scope, and Criteria 4
2. ISO 27001:2013 Framework 4
3. Scope of Audit 5
4. Audit Methodology 5
5. Category of Finding Rating 6
6. Summary of Internal Control Issues 6
7. Good Practice 6
8. Findings in Detail 7

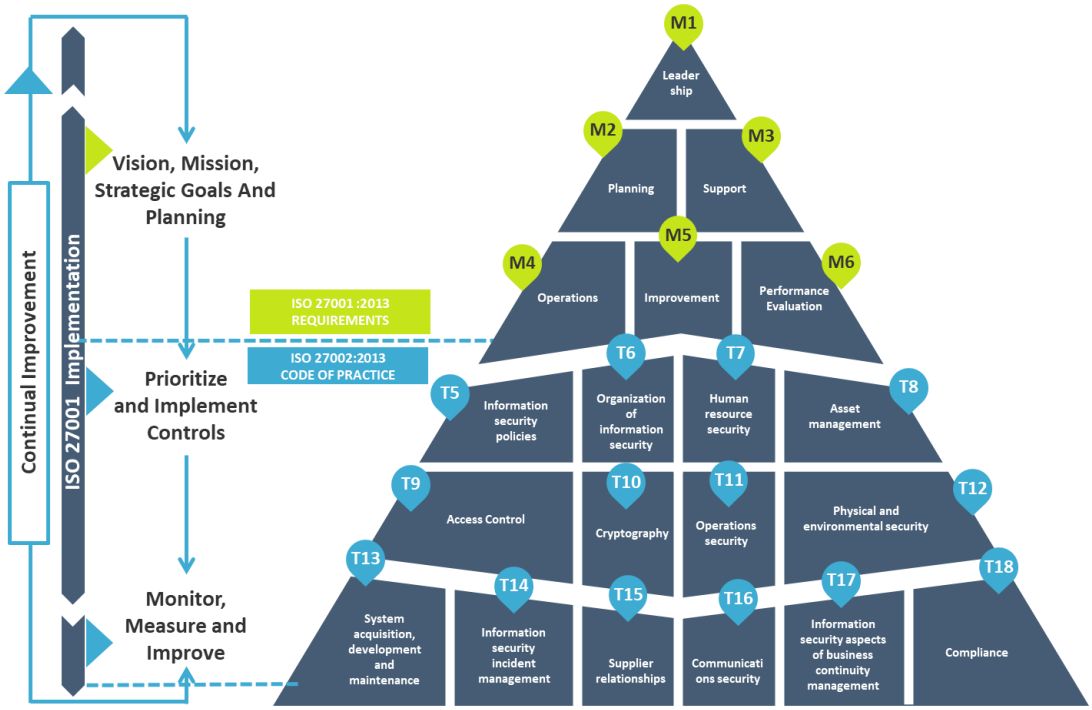
1. Assessment Objective, Scope, and Criteria

The objective of the internal audit was to conduct an internal assessment and look for positive evidence to ensure that elements of the scope of certification and the requirements of the management standard are effectively addressed by the organization's management system and that the system is demonstrating the ability to support the achievement of statutory, regulatory and contractual requirements and the organization's specified objectives, as applicable about the scope of the management standard, and to confirm the ongoing achievement and applicability of the forward strategic plan and where applicable to identify potential areas for improvement of the management system.

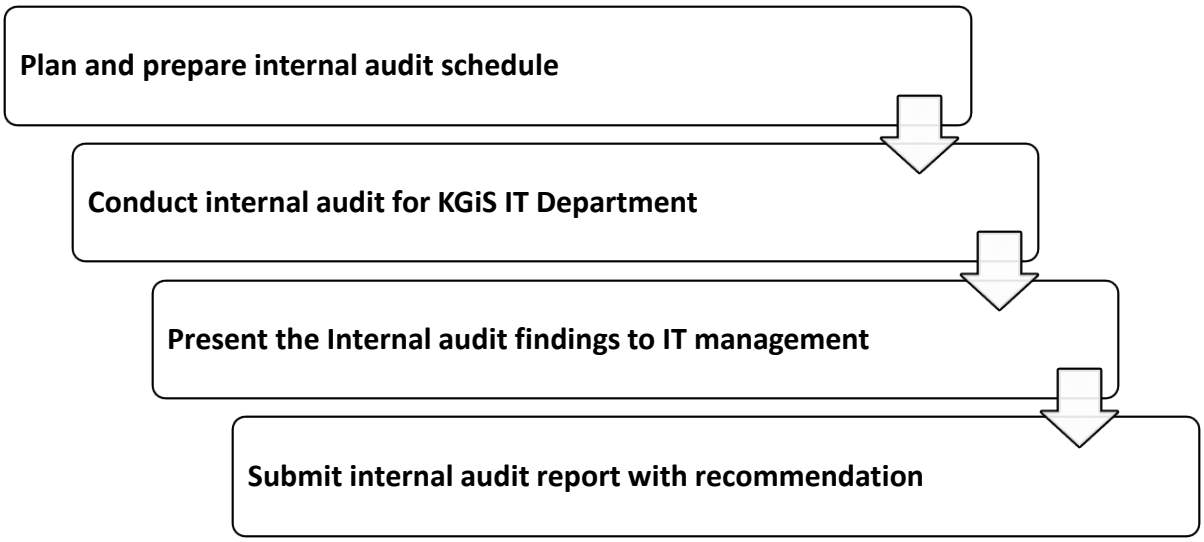
The scope of the assessment is the documented management system in relation to the requirements of ISO 27001:2013.

2. ISO 27001:2013 Standard

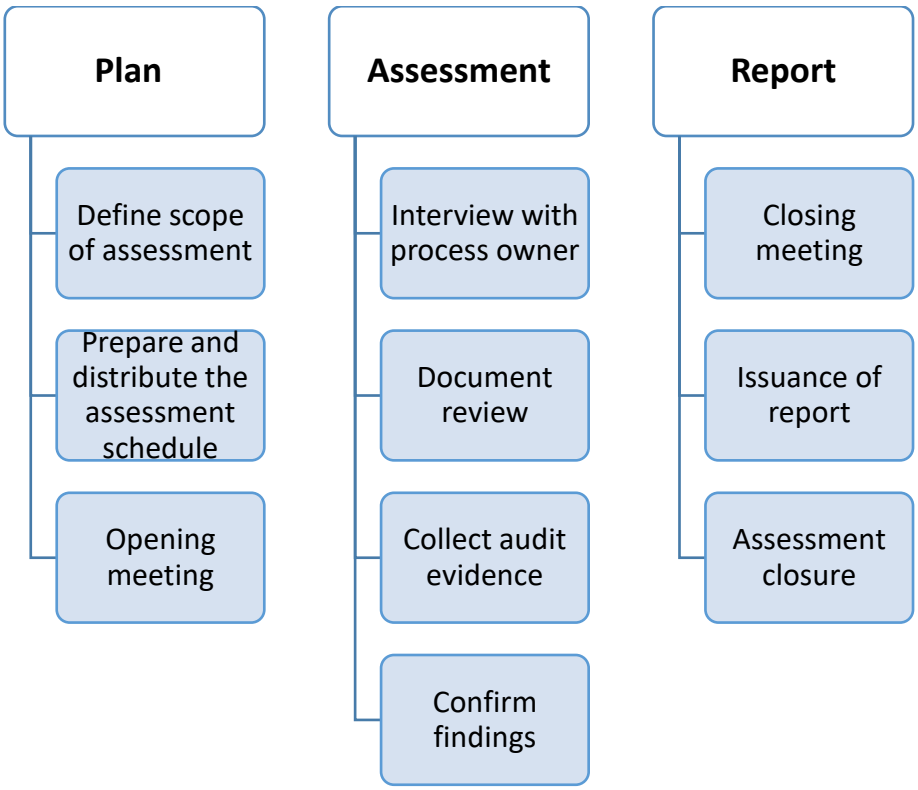
The below diagram represents the requirements of ISO 27001:2013 standard.



3. Scope of Audit



4. Audit Methodology



5. Category of Finding Rating

Category	Description
Major Non-Conformance (Major NC)	A breakdown or failure to fulfil one or more requirements of standard requirements to effectively control the processes, for which it was intended.
Minor Non-Conformance (Minor NC)	A single identified lapse, which would not in itself raise significant doubt as to the capability of the management system to achieve the Management System policy compliance and objectives of the organization.
Observation	Minor deviation and to improve upon the management system process that is already in place.

6. Summary of Internal Control Issues

We have assessed specific compliance risks identified within each area of scope, evaluated the associated mitigating controls, and commented on the results of our audit procedures. The non-conformity, Observations, Opportunities for Improvement, and Recommendations on the following pages are intended to provide guidelines for improving the existing controls over compliance risks and to improve the efficiency of current operating procedures.

Our review covered the period from 23rd May – 25th May 2023. The evidence was collected by interviewing, observing, reports, policies, and procedures.

This report is intended solely for the information and use of management of KGiS IT only and is not to be used or relied upon by any other party for any purpose.

7. Good Practice

1. Effective Backup management for the critical infrastructure system components.
2. Matured End -point security controls.
3. Management commitment towards cyber security compliance.
4. Well defined IT Infrastructure asset inventory (list of hardware and software components including description of functions/use of each)
5. The vulnerability assessment and effective tracking the closure of the vulnerabilities.

8. Findings in Detail

Unavailability of Approved Software list		Observation
Observation	Risk	Recommendation
List of approved software list is not maintained and approved by KGiS Information security team.	Un-approved software shall be installed on the endpoint and non-clarity on list of approved and un-approved software.	Approved software list shall be maintained
Agreed Management Action Plan:	The software inventory will be briefly captured with additional information like purchasing date, EOL, No. of License.	
Timeline:	June -2023	
Owner:	IT Department	

Un-availability of Mandatory ISO 27001 Documentation		Minor NC
Observation	Risk	Recommendation
KGiS has documented ISMS Documentation, however following document is missing as required by ISO 27001 standard 1. ISO 27001 Scope document 2. Information Security Risk Management Framework. 3. Information Classification and Handling procedure 4. Control of Document and Record procedure. 5. Internal audit and Corrective action procedure	ISO 27001 Non-Conformity / Failure to achieve compliance to ISO 27001	We recommend KGIS IT Department to document the ISMS mandatory documents.
Agreed Management Action Plan:	ISMS Mandatory documents will be documented in KGiS documentation template, and it will be approved by IT Management	
Timeline:	June -2023	
Owner:	IT Department – Information Security	

Unavailability of Web application firewall (WAF) for External facing application		Observation
Observation	Risk	Recommendation
Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification. During our audit we noted the following: Web Application firewall is not implemented to protect external web application from 10 Top OWASAP vulnerabilities.	Compromise of web application	We recommend KGIS IT Department to Implement Web Application firewall (WAF) for all external application to prevent cyber-attacks and compromise of applications.
Agreed Management Action Plan:	WAF related risk has been identified in many due diligence sessions. WAF will be enabled for the external facing application.	
Timeline:	Q4- 2023	
Owner:	IT Department – Information Security	

Inadequate security hardening guidelines and implementation		Observation
Observation	Risk	Recommendation
Minimum Security Hardening documents as per international security best practices such as CIS, STIG. NIST etc are not documented for Network, Security devices, Operating Systems, Databases, Applications, and other applicable IT Components	Theft or compromised of critical information and systems	We recommend KGIS IT Department the following: 1. Implement the Minimum-Security Hardening documents as per international security best practices such as CIS, STIG. NIST etc for Network, Security devices, Operating Systems, Databases, Applications, and other applicable IT Components 2. Implement Automated solution to measure the effectiveness of the implemented the Minimum-Security Hardening guideline.
Agreed Management Action Plan:	Minimum Security Hardening for windows OS will be implemented.	
Timeline:	August -2023	
Owner:	IT Department – Information Security	

Inadequate Security Requirements During Development		Observation
Observation	Risk	Recommendation
Information security requirements are not defined and documented during internal application development.	Non-Compliance to ISO standard requirement and leads to data breach.	We recommend KGIS IT Department to define, document and test the security controls during the lifecycle of software/application development. Security acceptance criteria needs to be developed by Infosec team for all new developed application.
Agreed Management Action Plan:	Information security team will start defining the security requirements during the development of internal applications.	
Timeline:	Q3- 2024	
Owner:	IT Department – Information Security	

****End of Document****