Information Security Risk Management Framework

KG Invicta Services (KGiS)

[Ref: ISMS-FWK-DOC-06]
[Ver: 1.0]
[05th April 2023]
[Classification: Internal]

+91 422 4419999

KGiS
o 365, KG Invicta Services Private Limited KGiS 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 Except with a prior written permission of KGiS, this document and the information contained herein may not be published, disclosed, or used for any other purpose.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 framework. 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 framework	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
Consequence	Refers to the outcome of an event.
Control	means the measure taken to diminish the probability and impact of associated risk.
Enterprise Risk Management System (ERMS)	the system within which risk information will be contained and maintained.
Establishing context	Defining the external and internal parameters to be taken into account when managing risk and setting the scope and risk criteria for risk management.
External context	external environment in which the organization seeks to achieve its objectives.
Internal context	internal environment in which the organization seeks to achieve its objectives.
Likelihood	Refers to the probability of something happening.
Monitoring	Refers to the continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected.
ISO	International Organization for Standardization.
Level of risk	It is the magnitude of a risk or combination of risks, expressed in terms of the combination of consequence and their likelihood.
Residual risk	It is the risk remaining after risk treatment.
Risk	Risk is the probability of occurrence of an event which would have an adverse impact on business objectives. It is important that we manage risks in order to reduce the negative impact of risks and maximize our ability to realize potential opportunities.
Risk analysis	Refers to the process of comprehending the nature of risk and to determine the level of risk.
Risk appetite	Refers to the amount of risk that KGiS is prepared to accept or be exposed to at any point in time.
Risk assessment	Refers to the overall process of risk identification, risk analysis and evaluation.

Risk evaluation	Refers to the process of comparing risk analysis with risk criteria to determine whether the risk and/or its magnitude are acceptable or tolerable.
Risk identification	finding, recognizing and describing risks.
Risk management framework	It is the set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization.
Risk management process:	Refers to the systematic application of management policies, framework and practices to the activities of communicating, consulting, establishing the context, identifying, analyzing, evaluating, treating, monitoring and reviewing risk.
Risk management	Coordinated activities to direct and control an organization with regard to risk.
Risk owner	Refers to the person or entity with the accountability and authority to manage a risk.
Risk treatment	means the selection and implementation of appropriate controls for dealing with risk.
Risk Source	Element, which alone or in combination has the intrinsic potential to give rise to risk.

3 About the Document

3.1 Introduction

Information Security Risk Management Framework (ISRMF) is a systematic approach that organizations follow to identify, assess, and mitigate risks to their information assets. It provides a structured process for managing risks to ensure the confidentiality, integrity, and availability of critical information.

The primary goal of an ISRMF is to enable organizations to make informed decisions regarding the allocation of resources and implementation of controls to manage information security risks effectively. By following a standardized framework, organizations can establish a consistent and repeatable process for managing risks throughout their information systems and infrastructure.

In addition, it identifies other key activities needed for an effective risk management approach. The risk management process contained in this procedure aligns with the Standard for Risk Management (ISO31000:2009).

3.2 Objective

The primary objective of an Information Security Risk Management Framework is to effectively manage risks to an organization's information assets.

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

- Head of ICT is responsible to approve this procedure and to ensure that it reflects the current requirements.
- Information Security Officer is responsible for performing risk assessment annually or whenever required.
- Head of ICT are responsible for compliance to the Information Security Risk Management Framework within their own area(s) of operations.
- Employees, Contractors, and Third Parties are responsible for understanding and aligning their activities with the Information Security Risk Management Framework.
- Information Security Officer is responsible for reviewing the Information Security Risk Management Framework on a periodic basis to ensure their continuing suitability, adequacy, and effectiveness.
- Internal Audit Team is responsible for conducting regular audits to ensure compliance to this procedure.

4 Procedure

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

Information Security Risk management is a continual process that involves the following key steps:

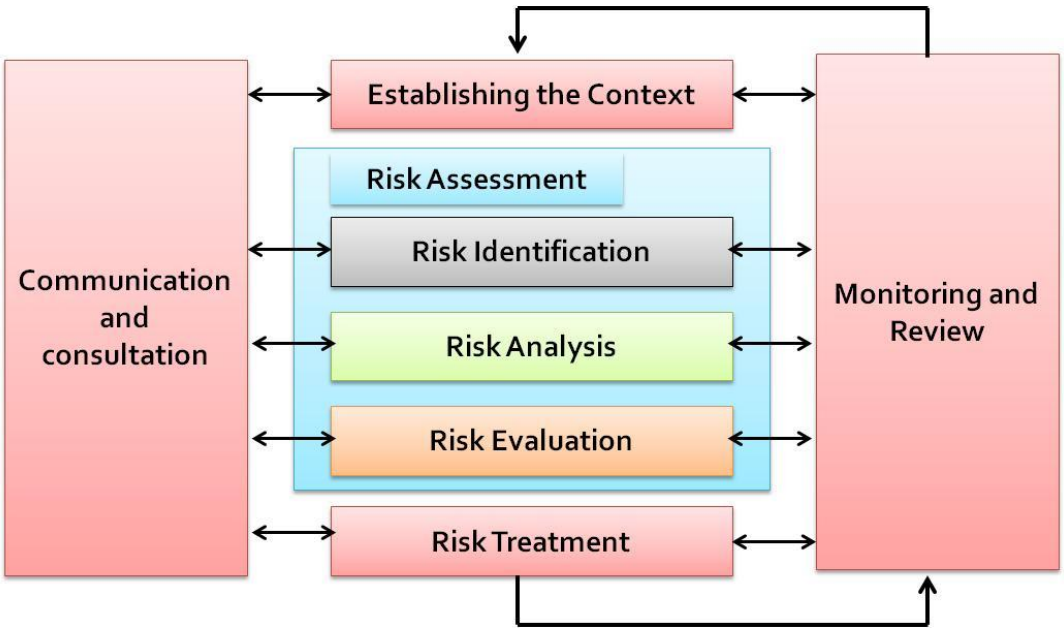

Figure 1 - Risk Management

- Communication and consultation
- Establish the context
- Identify risks
- Analyze risks
- Evaluate risks
- Treat risks
- Monitor and review.

It is important to follow this process when conducting risk management as this ensures that the KGiS - ICT approach to risk management is both comprehensive and consistent.

This process is formally conducted across KGIS ICT on an annual basis or when significant changes are proposed or occur. This occurs in conjunction with the corporate and business planning process and involves the review and update of risk profiles for the enterprise as a whole includes a review for each individual division. This illustrates a "top-down" and a "bottom-up" approach to risk management. Although this process is conducted across the entire organization on an annual basis, risk management is not solely an annual process. It should be occurring at all times and in relation

to all business activities. Therefore, everyone has a responsibility to continually apply this process when making business decisions and when conducting day-to-day management.

To assist you in completing the risk management process, each process step is described in further detail.

4.1 Communication and Consulting

- Effective communication, consultation and education in risk management are necessary to achieve a successful integration of the risk processes into the business.
- Communication and consultation with internal and external stakeholders are important throughout the risk management process to ensure the organization has a comprehensive picture of the risks they face.
- External communication and consultation are targeted at informing external stakeholders of:
    - The organization's risk management approach
    - The effectiveness of our risk management approach.
    - Requesting feedback where appropriate.
- Risk management is key governance and management function, which external stakeholders, including government and industry, are, paying, increased attention to. Satisfying these stakeholders that we use appropriate risk management practices will influence their perception of the organization.
- Internal communication and consultation are aimed at informing internal stakeholders of:
    - The risk management process.
    - Seeking feedback in relation to the process.
    - Key risks and their responsibilities relating to management of these.

4.1.1 Establishing The Context

- KGiS ICT Department considers both external and internal factors when identifying and managing risks associated with the achievement of strategic and operational objectives.

The external context

- Building an understanding of our external stakeholders and hence, the extent to which this external environment will impact on our ability to achieve corporate objectives:
    - Business, Social, Regulatory, and Financial Environments in which KGiS operates.
    - It also involves considering our strengths, weaknesses, opportunities and threats; and
    - Relationships with perceptions and values of external stakeholders.

The internal context

- This is aimed at understanding organizational elements and the way they interact, such as:
    - Governance, organizational structure, roles and accountabilities.
    - Policies, objectives, and the strategies that are in place to achieve them.
    - The capabilities, understood in terms of resources and knowledge (e.g., capital, time, people, processes, systems and technology)
    - Information systems, information flows and decision-making processes (both formal and informal).
    - Relationships with, and perceptions and values of, internal stakeholders.
    - The organization's culture.
    - Standards, guidelines and models adopted by the organization; and
    - Form and extent of contractual relationships.

The risk management context

- The goals, objectives, strategies, scope and parameters for the risk management process itself must also be considered.

Note: The "Establish the Context" part of the risk management process only needs to be repeated when there are significant changes to either our external environment or business operations.

4.1.2 Identify Risk

KGiS ICT Department identifies risk sources, areas of impacts, events, causes and possible consequences to form a comprehensive list of risks based on those events that might prevent, or delay the achievement of objectives.

Risk identification is a key step in the risk management process to ensure a complete list of risks is identified. Risk identification uses below mentioned sources to capture the possible risks to the organization.

- Documented Risk Register;
- Policy and Procedure review;
- Interview with department heads;
- Control weaknesses identified in Gap Assessment report;
- Vulnerability Assessment and Penetration Testing report; and
- Additional requirements of Internal and External stakeholders.

Identifying all elements provides a better understanding of the risk and assists when considering current controls and identifying further treatment actions. It also reduces risk duplication and minimizes confusion about risk meaning.

Following information about risk is captured during risk Identification:

- Risk ID (E.g. SG-01 for Strategy Risk)
- Date of identification of risk
- Relevant ICT responsible resource to handle the risk
- Services affected by the risk
- Information Asset on which the risk is applicable
- Vulnerabilities associated with the risk
- Threats which can expose the vulnerabilities
- Risk Context (whether the risk is Internal or External risk)
- Risk Owner

4.1.3 Risk Analyze and Evaluate

- Risk analysis means considering the range of causes, sources of risk, consequences and likelihood to produce a risk rating. The rating can then be used to determine further risk treatment plans by KGis ICT Department.

  Risk Analysis involves:

  - Identify the inherent risks;
  - Identifying controls currently in place to manage the risk by either reducing the consequence or likelihood of the risk;
  - Assessing the effectiveness of current controls;
  - Identifying the likelihood of the risk occurring; and
  - Identifying the potential consequence or impact that would result if the risk occurs.
- When evaluating the effectiveness of current controls, the factors to consider include consistency of application, understanding of control content and documentation of controls where appropriate. Controls are aimed at bringing the risk within an acceptable level. The evaluation of current controls can occur through several different processes including:
  - Control self-assessment;
  - Internal Audit reviewing the effectiveness of controls; and
  - External Audit reviewing the effectiveness of controls.
- The consequence and likelihood ratings, as identified after consideration of current controls, are combined to determine the overall risk level.

Risk Evaluation Criteria			
Likelihood			
Frequent (3)	Low 3	Medium 6	High 9
Possible (2)	Low 2	Medium 4	Medium 6
Rare (1)	Low 1	Low 2	Low 3
	(1) Incidental	(2) Moderate	(3) Major
	Impact/Consequences		

Figure 2 Risk Evaluation Criteria

Likelihood	
RATING	POTENTIAL FOR RISK TO OCCUR
Frequent	The risk event is expected to occur more than once per quarter
Possible	The risk event is expected to occur at least once per year
Rare	The risk event is expected to occur at least once in 2 years

Figure 3 Likelihood Rating

Consequences/Impact	
The potential outcome of a risk event that affects an organization's business objectives on the assumption that an event has occurred and the most probable consequence has resulted rather than the worst-case scenario.	
RATING	POTENTIAL FOR RISK TO OCCUR
Major	The loss of confidentiality, integrity, or availability could be expected to have a major adverse effect on KGIS operations, KGIS assets or individuals
Moderate	The loss of confidentiality, integrity, or availability could be expected to have a moderate adverse effect on KGIS operations, KGIS assets or individuals.
Incidental	The loss of confidentiality, integrity, or availability could be expected to have a no adverse effect on KGIS operations, KGIS assets or individuals.

Figure 4 Consequences / Impact

Control Assessment			
Any action or activity that the Organization has in place that either reduces the likelihood of a risk event occurring or minimizes the potential for impact arising from that event.			
Rating	Design	Performance	Overall Control Assessment
Effective	Designed to reduce risk entirely	Control is always applied as intended	The design and the performance of the controls are considered sufficient
Adequate	Designed to reduce most aspects of risk	Control is generally operational but on occasions is not applied as intended	Minor weaknesses exist in the design or in the performance of the control
Marginal	Designed to reduce some area of risk	Control is sometimes applied correctly	Deficiencies exist in risk mitigation / controls
Deficient	Very limited or badly designed, even where used correctly provides little or no protection	Control is not applied or applied incorrectly	Fundamental deficiencies exist in risk mitigation / controls

Figure 5 Control Assessment

Risk Evaluation involves:

- Risk evaluation means the ranking and prioritization of level of identified risks, according to a consistent overall ranking and rating system.
- Below table depicts the Risk Level based on likelihood, consequence of the risk.

Risk Levels	
High – Need Action	6-9
Moderate – Need Attention	3-6
Low – Monitoring Needed	1-3

Risk Level (potential / residual) = Likelihood * Consequence/Impact

Risk Treatment Option	
Depending on the type and nature of the risk, the following options are available:	
Option	Treatment
Avoid	A strategy to control risk by eliminating the possibility of loss by exiting any activity that would expose the company/project/ business unit to a loss (e.g... using alternate systems, applications, processes etc.)
Accept	A strategy to defer action and maintain the current impact and probability of a risk until it rises above an acceptable level
Mitigate	A strategy to reduce the probability and/or negative impact of a risk to an acceptable level (e.g. Training)
Share/Transfer	A strategy to remove the risk from the risk portfolio by eliminating risk drivers and activities (e.g. Insurance)
Exploit	A strategy to develop a competitive advantage by capitalizing on the company's expertise around a risk and thereby turning the risk into an opportunity

There may be times when the action required will differ from that identified above; however where this is the case, the Chief Executive Officer must approve deviation from the above action.

4.1.4 Treat Risk

Risk treatment involves developing a range of options for mitigating the risk, assessing those options, and then preparing and implementing action plans. The highest rated risks should be addressed as a matter of urgency.

Risk treatments steps include;

- Developing a risk treatment Plan
- Documenting the treatment plan
- Assigning risk owner
- Specifying target resolution date

Note: Low Level Risks are acceptable risks as per the risk management framework.

4.2 Monitor and Review

Continual monitoring and reviewing risk profiles is essential to maintain the effectiveness and appropriateness of KGiS Department's risk management profiles, including more specifically, risk treatment plans, risk assessments and to identify emerging risks.

Monitoring and review should be a planned part of the risk management process and involve regular checking or surveillance. The results should be recorded and reported externally and internally, as appropriate. The results should also be an input to the review and continuous improvement of the Organization's risk management framework.

Information Security Officer monitors and reviews ICT risk management framework and risk register annually or any significant changes. KGiS ICT monitoring and review processes encompass all aspects of the risk management process for the purposes of:

- Ensuring that controls are effective and efficient in both design and operation;
- Obtaining further information to improve risk assessment;
- Analyzing and learning lessons from risk events, including near-misses, changes, trends, successes and failures;
- Detecting changes in the external and internal context, including changes to risk criteria and to the risks, which may require revision of risk treatments and priorities; and
- Identifying emerging risks.

The identified risks in the organization's risk register should be regularly reviewed. Document any actions or events that change the status of a risk, for example:

- Changes to a risk evaluation as a result of improvements in controls
- A control breach and near miss should be logged at the time of the event
- A new risk that has been identified.

ISSC should review the risk register on a regular basis, at regular ISSC meetings, to determine if any remedial action needs to be taken immediately.

4.3 Risk Identification and review

- Risk may be detected by anybody within KGiS department. The concerned personnel shall immediately bring it to the notice of the Information Security Officer.
- The Information Security officer shall perform risk analyze, evaluate and treat the risk appropriately and communicate the status to the user.

4.4 Review and Approval

The Information Security Risk Management Framework and report templates will be reviewed annually by the KGiS Information Security Office.

4.5 Risk Assessment Template

Risk Assessment template _v1.0_Final.x