# Information Security Management System
## Risk Management Methodology

Document No. - JMBGRP/ISMS/Apex_04

Version_v1.2

## Document Details

| | | |
|---|---|---|
| **Classification** | Internal | |
| **Released date** | 28.08.2018 | |
| **Description** | The documented policy and methodology for addressing and assessing the risks to JMBGRP's Information and processing facility. | |
| **Custodian** | Corporate IT dept. | |
| **Approved by** | Manish Jaiswal (Group CTO) | |
| **Owner** | Corporate IT Dept. | |

## Distribution List

| **Name** |
|---|
| To JMBGRP Employees Only |
| Third Party and Auditors: On Need basis |

## Version History

| **Version no.** | **Version date** | **Approved by** | **Comments** | **Signature** |
|---|---|---|---|---|
| v1.0 | 28.08.2018 | Manish Jaiswal (Group CTO) | Reviewed & no changes | |
| v1.0 | 10.01.2019 | Manish Jaiswal (Group CTO) | Reviewed & no changes | |
| v1.0 | 08.02.2020 | Manish Jaiswal (Group CTO) | Reviewed & no changes | |
| v1.0 | 11.02.2021 | Manish Jaiswal (Group CTO) | Reviewed & no changes | |
| v1.1 | 25.03.2022 | Manish Jaiswal (Group CTO) | Logo changes done in this policy | |
| v1.2 | 18.08.2023 | Manish Jaiswal (Group CTO) | Document reviewed. Modification done to "11. Reference to ISO 27001:2022" | |
| v1.3 | 16.10.2024 | Manish Jaiswal (Group CTO) | Modifications done in Section: "9" | |

# Contents

# 1. Introduction

**1.1.** J.M Baxi Group (JMBGRP) is aligning with the ISO 27001:2022 Standard and integrating a risk management methodology based on ISO 31000:2018 to assess risks associated with its information and processing assets.

**1.2.** This document aims to delineate the policy and methodology governing risk assessment for JMBGRP's information infrastructure, emphasizing the significance of adhering to internationally recognized standards. By adopting ISO 27001:2022 and ISO 31000:2018, JMBGRP seeks to effectively mitigate risks and enhance the resilience of its operations. The methodology outlined herein outlines procedures for identifying, analyzing, evaluating, and treating risks across all organizational dimensions, emphasizing proactive risk management as fundamental to JMBGRP's commitment to information security and governance excellence. In essence, the integration of ISO standards provides a structured approach for JMBGRP to systematically manage risks and uphold the confidentiality, integrity, and availability of its information assets.

# 2. Purpose and Scope

**2.1.** The purpose of the Risk Management Methodology is to evaluate the risk associated with identified threats and vulnerabilities pertaining to specific information assets by implementing existing controls and potentially introducing security measures.

**2.2.** This policy encompasses all information assets and intellectual property with potential business implications if compromised. These assets include digital and non-digital documents stored across various media such as CDs, DVDs, tapes, and hard disks. Additionally, it covers other resources like network infrastructure equipment, software, applications, services, and supporting utilities such as electrical supply, UPS systems, air- conditioning, and power substations utilized by J.M Baxi Group (JMBGRP), whether on its premises or external locations in collaboration with third-party entities under contractual agreements with JMBGRP.

# 3. Normative Reference

**3.1.** **ISO 31000:2018**, Risk Management Guidelines.

**3.2.** **ISO 27001: 2022**

**3.2.1. Clauses:** 6.1.2, 6.1.3, 8.2 & 8.3

**3.2.2. Controls**: A.5.9, A.5.12, A.5.13, A.7.9

## 4. Terms and Definition

For this document, terms and definition are defined in Annexure 8.

## 5. Policies

**5.1** This policy aims to establish a risk management framework tailored to and aligned with the specific business needs of J.M Baxi Group (JMBGRP).

**5.2** The risk management and mitigation efforts of JMBGRP shall encompass information security risks associated with identified Information Assets, spanning business operations, vendors, and compliance with regulatory and legal mandates.

**5.3** JMBGRP will establish a formal process for conducting Risk Assessments (RA) and implementing Risk Treatment Plans (RTP) for all identified assets, both on its premises and those held by vendors.

**5.4** Risk assessment will consider the following factors:

**5.4.1.** The potential business impact resulting from the occurrence of the threat.

**5.4.2.** The likelihood of the threat occurring.

**5.4.3.** Risk Impact Rating which is defined as:

**Asset value * Severity of Threat * Probability or Likelihood of risk development and implemented**

**Note**: This rating will guide the establishment of an acceptable level of risk.

**5.5.** Risk Treatment Plan shall consider all the aspect of Risk Treatment i.e. Acceptance, Avoidance, Mitigation, Transfer (Defined in annexure).

**5.6.** The responsibility for the execution, development, and implementation of Risk Assessment and Risk Treatment Plans lies with the Head of Department (HOD) and the designated Risk Manager or Designated Individual (DR/DI) within each department.

**5.7.** A comprehensive **Risk Register** shall be maintained and adhered to, serving as a central repository for efficient risk assessment and storage of pertinent information essential for the development and implementation of risk treatment strategies.

**5.8.** JMBGRP is committed to developing and/or implementing appropriate controls to mitigate information security risks to a level deemed acceptable in alignment with the organization's risk appetite. Any residual risks remaining after the implementation of primary controls shall be evaluated, and supplementary controls may be applied to ensure they remain within acceptable limits for JMBGRP.

**5.9.** Periodic review of the Risk Assessment and Risk Treatment shall be conducted to account for significant changes in the business environment, organizational structure, and regulatory landscape that may impact the information security posture of JMBGRP.

**5.10.** The effectiveness of the Risk Assessment and Risk Treatment approach shall be measured through the development of appropriate metrics, which will be reviewed periodically to ensure their relevance and adequacy.

**5.11.** A formal process shall manage any exception to this policy.

## 6. Responsibilities

**6.1** The responsibility of ensuring that this document is maintained up-to-date and approved by the Apex Committee.

**6.2** The following shall be responsible for governing the Risk Management Plan.

**6.2.1.** **Senior management** is responsible for establishing, maintaining, and continually improving the risk management framework within JMBGRP. This includes providing necessary resources, support, and leadership to ensure effective risk management practices are implemented across all levels of the organization.

**6.2.2.** **HODs** are accountable for overseeing risk management activities within their respective departments. This involves identifying department-specific risks, implementing appropriate controls, and regularly reviewing risk assessment findings to ensure compliance with organizational policies and objectives.

**6.2.3.** **Risk Managers/Designated Individuals** (RM/DIs): These individuals are responsible for facilitating the execution, development, and implementation of risk assessment and treatment plans within their departments. They collaborate closely with HODs to ensure that risks are adequately identified, evaluated, and managed according to established procedures.

## 7. Methodology

The procedure details the risk assessment and risk treatment with templates and certain definitions and terminologies, which shall contribute towards better understanding of the process. Procedure includes:

**7.1.** Identification of Assets.

**7.2.** Evaluation of assets value.

**7.3.** Risk Assessment

**7.4.** Risk Treatment

**7.5.** Reporting.

**Note:** The entire procedure and practices are mentioned in 9.0 Risk Management Procedure.

## 8. Risk Ownership and responsibilities.

The purpose of this policy is to define the roles and responsibilities related to risk ownership within JMBGRP, ensuring clear accountability and effective risk management practices throughout the organization.

**8.1. Definition:**

**8.1.1.** **Risk Owner:** An individual or entity assigned the responsibility for overseeing and managing a specific risk within the organization.

**8.1.2.** **Risk Responsibility:** The obligations and duties associated with identifying, assessing, mitigating, and monitoring risks, as well as reporting on risk-related matters.

**8.2.** The Risk Owner shall assume responsibility for the treatment and management of identified risks, including the acceptance of residual information security risks.

**8.3.** The Risk Owner is tasked with developing a comprehensive mitigation plan to address identified risks and overseeing its implementation.

**8.4.** The Risk Owner is expected to actively support and participate in the execution of the mitigation plan, taking visible steps to ensure its effectiveness.

**8.5.** The Risk Owner must maintain a thorough understanding of the organization's business objectives, with specific emphasis on the utilization of internal and external information assets.

**8.6.** It is imperative for the Risk Owner to comprehend the information security risks faced by the organization and its business partners, taking necessary measures to address them effectively.

**8.7.** The Risk Owner shall communicate investment implications, including outsourcing decisions, related to identified risks to the management for informed decision-making.

**8.8.** The Risk Owner shall regularly report on the status of assigned risks to relevant stakeholders, including updates on risk assessments, mitigation efforts, and any significant changes in risk exposure.

## 9. Risk Management Procedure.

**9.1. Asset analysis**.

**9.1.1. Name of Information Asset:**

This consists Title/name/Category of the information asset.

### 9.1.2. Asset Categorization:

The nature of the asset, whether it is Information in Soft Copy or Hard copy, Software & Application, Service, Physical Asset (Hardware) or People need to be mentioned. The definitions of different types of assets have been illustrated in Annexure 1.

### 9.1.3. CIA Triad

This is a matrix from which the criticality of the asset is evaluated individually.
The average of the confidentiality, Integrity and Availability is taken for evaluation.

### 9.1.4. Business Impact Criteria:

The potential impact on JMBGRP's business, including financial implications, disruption to operations, damage to brand reputation, and legal or regulatory compliance concerns, is assessed if an information asset or intellectual property is compromised. Ratings of very high, high, medium, low, and very low, assigned values of 5, 4, 3, 2, and 1 respectively, are used to evaluate the severity of these impacts. Further details regarding the specific criteria and their definitions are provided in Annexure 2. Additionally, the cumulative ratings for business impact criteria are totaled to derive the "Total Score.

### 9.1.5. Asset classification:

The asset classification shall be done based on the Confidentiality parameter compromise:

**9.1.5.1.** SECRET

**9.1.5.2.** CONFIDENTAIL

**9.1.5.3.** INTERNAL

**9.1.5.4.** PUBLIC

**NOTE:** The details are mentioned in Annexure 3.

### 9.1.6. Asset value:

Asset value is evaluated as the average of score of Confidentiality, Integrity, and Availability.

**9.1.6.1.** If total score is <=20 & >=13 then, **"CRITICAL",** Asset Value = 4

**9.1.6.2.** If total score is <=12 & >=9 then, **"IMPORTANT",** Asset Value = 3

**9.1.6.3.** If total score is <=8 & >=5 then, **"GENRAL",** Asset Value = 2

**9.1.6.4.** If total score is <=4 then, **"NEGLIGIBLE",** Asset Value = 1

Risk assessment needs to be done for all the assets identified as **CRITICAL** and **IMPORTANT** during asset valuation.

### 9.1.7. Asset Owner:

In the context of this policy, the term 'owner' refers to an individual or entity entrusted with management responsibility for overseeing the production, development, maintenance, utilization, and security of the asset. Owners establish the security protocols for information assets and are tasked with communicating these requirements to all **custodians** responsible for the assets.

**Note: Custodians** are the authorized entities/ people who can have the custody of the said Information Asset

## 9.2. Risk Assessment

**9.2.1.** The following Template is used as asset inventory.

| Loss of Integrity | | | | | Asset Classification | Loss of Availability/ Criticality/Essentialness | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Financial Impact | Operations/ Processes | Brand / Reputational | Legal/ Regulatory/ Compliance | Total Score for Loss of "I" | RESTRICTED CONFIDENTIAL INTERNAL PUBLIC | Financial Impact | Operations / Processes | Brand / Reputational | Legal/ Regulatory/ Compliance | Total Score for Loss of "A" |
| | | | | | | | | | | |

| Sr.No. | Information Asset | Type of Information Asset | | | | | | Loss of Confidentiality/ Sensitivity to disclosure | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Soft copy | Hard copy | Software | Physical | Service | People | Financial impact | Operations /Processes | Brand/ Reputational | Legal/ Regulatory/ Compliance | Total Score for Loss of "C" |
| | | | | | | | | | | | | |

| Avg. of CIA | Asset Value | Risk Assessment | Information Asset Ownership | |
|---|---|---|---|---|
| | 4- Critical 3- Important 2- General 1- Negligible | Required (YES FOR "Critical" AND "Important" Asset Value) | Owner | Custodians |
| | | | | |

**9.2.2.** The following template is used for Risk Assessment and Treatment Collectively.

| Sr. No. | Asset Value | Compromise Parameters | Threat | Severity of threat (S) 1,2,3,4,5 | Vulnerability | Likelihood of occurrence (P) 1,2,3,4,5 | Risk Impact Rating RIR = AV*S*P | Risk Treatment Required ? | Departments where gaps were observed |
|---|---|---|---|---|---|---|---|---|---|
| **Soft Copy - Critical** | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

| Existing Control | Risk Treatment Options | Recommended Control | Mapping with ISO27001:2013 | Responsibility / Risk owner | Timeline | Severity of threat (S) 1,2,3,4 | Likelihood of occurrence (P) 1,2,3,4 | Residual RIR = AV*S*P | Management Approval |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

The Above Table is used for the Risk Assessment and Treatment and provides with the structural approach to address any risk or Threat within the organization.

### 9.2.3. Severity of the Threat

| Severity of Threat | | | | |
|---|---|---|---|---|
| 1- Very Low | 2- Low | 3- Medium | 4- High | 5- Very High |

When evaluating the Severity of Threat rating, the following factors should be considered:

**9.2.3.1. Financial Impact:** Potential loss of sales, loss of profitability, or imposition of pecuniary penalties and/or impact on share price.

**9.2.3.2. Disruption to Business Operations / Process (es):** Potential disruption to business operations/ process (es) such as failure to deliver products or services

**9.2.3.3. Brand / Reputational:** Potential negative public (press, customer or government) exposure, employee reaction and/or loss of business relationship(s).

**9.2.3.4. Legal & Regulatory Compliance:** Potential impact on compliance with industry standards or government regulations including oversight by industry or government and/or restriction(s) on business operation

**9.2.3.5.** Severity of the threat is function of C, I and A which indicates the impact that asset or group of assets will have, if compromised. The below scale shall be used to determine the severity of any threat as shown in Annexure 4.

**9.2.4.** Likelihood of Occurrence of Threat (P):

| Likelihood | | | | |
|---|---|---|---|---|
| 1- Very Low | 2- Low | 3- Medium | 4- High | 5- Very High |

When evaluating the likelihood rating, the following factors should be considered:

**9.2.4.1** Existence of a vulnerability or set of vulnerabilities.

**9.2.4.2** Existence of security control or set of controls.

**9.2.4.3** The extent to which vulnerability is discoverable/ identifiable.

**9.2.4.4** Likelihood that a threat will exploit a given vulnerability (i.e., access vector, access complexity).

**9.2.4.5** Technical vulnerability severity rating.

**9.2.4.6** Environmental context.

**9.2.4.7** The owner of an asset shall assign a rating to likelihood of occurrence of the threat on a scale of 1 to 5.

**9.2.4.8** Likelihood of Occurrence shall be considered over a period of one year.

**9.2.4.9** Likelihood of Occurrence – Annexure 5

### 9.2.5 Risk matrix:

| Risk Matrix | Severity of Threat | | | | |
|---|---|---|---|---|---|
| **Likelihood** | **1- Very Low** | **2- Low** | **3- Medium** | **4- High** | **5- Very High** |
| **1- Very Low** | Low | Low | Low | Low | Low |
| **2- Low** | Low | Low | Low | Low | Medium |
| **3- Medium** | Low | Low | Low | Medium | High |
| **4- High** | Low | Low | Medium | High | Very High |
| **5- Very High** | Low | Medium | High | Very High | Very High |

### 9.2.6 Risk Impact Rating:

**9.2.6.1** Once the values for the severity and likelihood have been established, The Owner of an information asset shall calculate the Risk Impact Rating (RIR) for an information asset. RIR is a product of Asset Value based on classification, Severity of threat and likelihood of occurrence of threat.

**RIR= AV*S*P**

**RIR** – Risk Impact Rating

**AV** – Asset Value

**S** – Severity of Threat

**P** – Likelihood of Occurrence

**9.2.6.2** Severity of Threat is on scale of 1 to 5, Likelihood of Occurrence of threat is on scale of 1 to 5 and Asset Valuation is on scale of 1 to 4. RIR=AV*S*P (multiplication of all three parameters leads to possible values ranging from 1 to 100, threshold for risk treatment has been considered as 25 which contains most of the real risk values around it.

**9.2.6.3** For example: an agreement critical to operations AV=4 (Critical), severity of a fire incident inside a wooden cabinet without any fire protection or resistance will be high (4) and the likelihood of such incidents in the office area could be medium (3). Hence RIR= 4(AV) * 4(S) *3(P) = 48

**9.2.6.4** Severity of Threat and Likelihood of Occurrence Matrix and Risk Impact Rating: Please refer Annexure 6

## 9.2. Risk Treatment

**9.3.1.** A risk Treatment Plan shall be developed to prioritize and address the risks identified during the Risk assessment phase by way of appropriate risk treatment measures in the form of controls.

**9.3.2.** Management should take appropriate decisions on the acceptance or treatment

of the risk.

**9.3.3.** Acceptable level of Risk is a numeric value (threshold) such that if the risk impact rating (RIR) for an information asset with respect to a given threat (and associated vulnerability) is below this value, then the corresponding risk is acceptable and need not be treated

**9.3.4.** The Security In-charge and Apex Committee shall identify the Acceptable Level of Risk and Management shall approve the same. Once the decision has been taken on the requirement of treatment to the risk (based on the threshold value), the risk owner with consultation of Security In-charge shall select any of the risk treatment options from below:

**9.3.4.1. Risk Avoid:** This approach entails actively avoiding activities or circumstances that could lead to the occurrence of a risk. By ceasing or discontinuing certain business activities or processes, we eliminate the risk entirely.

**9.3.4.2. Risk Mitigate:** Mitigation strategies focus on reducing the likelihood or impact of identified risks. Through the implementation of controls, safeguards, or preventive measures, we seek to minimize the probability of risk occurrence or lessen its consequences.

**9.3.4.3. Risk Accept:** Acceptance acknowledges the existence of a risk without taking specific action to mitigate or transfer it. This approach is adopted when the cost or effort required to address the risk exceeds its potential impact or when it aligns with our predetermined risk tolerance levels.

**9.3.4.4. Risk Transfer:** Transfer involves shifting the responsibility for managing and bearing the consequences of a risk to another party. This can be achieved through insurance, contracts, or outsourcing agreements, thus mitigating our exposure to the risk.

**9.3.5. Residual risk:**

Residual risk is the risk left over after implementation of a risk treatment option (recommended controls). It is the risk remaining after exercising all of the possible options of treatment. The residual risk has to be accepted by the Risk Owner. For JMBGRP any risk having risk impact rating <25 shall be considered as residual risk and accepted. Any Risk having RIR >25 or equal to 25 shall be reviewed by Information Security Committee.

**9.3.5.1.** The Information Security team shall also identify the owner for control implementation with the timelines in which the risk has to be treated.

**9.3.5.2.** The Information Security Team shall follow up with the owner for the status of implementation regularly.

9.3.5.3. Review of Risk Assessment shall be done once every year or in case of any major changes to the department or in case of changes to the IAC, whichever is earlier, or based upon the inputs received from an internal or external audit or as per the business need, or based on the recommendations which emerge from the Security In-charge review which is done periodically. The Risk Review shall also be done

based upon the communication of new or emerging risks by the Security In-charge to the concerned department, change in the structure of a department, inclusion of new information assets in the department, change of regulatory posture or change in the external business environment or the bank's business.

**9.3.5.4.** The Security In-charge shall be responsible for getting management commitment for the same.

## 10. Periodic Review and Update

**10.1.** The periodic Risk Assessment review by the top management is an integral part of the ISMS for continual improvement. Any change taking place in the business model, organization structure, change in infrastructure, essentially calls for a management review of the risk assessment. The methodology document should also be reviewed when the risk assessment is being reviewed. The risk assessment and risk treatment must be reviewed at least once a year.

# 11. Annexure 1- Information Asset Classification

| Type of Assets | |
|---|---|
| **Soft Copy** | Any asset in electronic/Digital form shall be referred as Soft Copy. These assets are generally stored on computers, laptops, servers, media/tapes/mobiles etc.<br>Example: MS Excel sheets, MS Word documents, MS PowerPoint, MS Projects, PDF, .pst files, configurations, e-mails, messages, chats etc. |
| **Hard Copy** | Any document in tangible paper, hard copy, banner form shall be considered as hard information asset. Hard assets are stored in files, cabinets, shelves etc.<br>Example: Employee personal files, Agreements in hard copies, hoardings, banners, printouts, designs, charts, reports etc. |
| **Software** | This will include enterprise and production applications utilities, customized tools, mobile apps, and other packaged software.<br>Example: SAP, Operating Systems, Office suites, WinZip, SharePoint applications, mobile application, etc. |
| **Physical** | Any information system or information processing facility in tangible form will be referred as physical assets. Generally, this type comprises of the assets, which are used to facilitate the operations at Sanofi.<br>Example: Laptop, Servers, Firewall, Router, Switches, Printer, Scanner, Hard Disk, USBs, Backup Tapes, Security equipment like CCTV camera, biometric controls etc. |
| **Service** | Services are those utility operations and security operations, which are required to support the smooth running of above four categories.<br>Example: Power cabling, Fire security service, Physical security services, D.G. Set, UPS, Helpdesk Services, Warehouse, Audit, Archival used etc. |
| **People** | People assets may include employees, management, customers, contractors, subscribers, visitors, security guards, cleaning personal and any other person, which are required to process or used information, information processing facilities or provide services. |

## 12. Annexure 2- Business Impact Parameters

| | Confidentiality - Ensuring that information is accessible only to those authorized to have access. | | | | |
|---|---|---|---|---|---|
| **Business impact Parameters** | **Very High (5)** | **High (4)** | **Medium (3)** | **Low (2)** | **Very Low (1)** |
| **Financial Impact** | Compromise information asset may lead to a severe financial impact at a corporate level | Compromise information asset may lead to high financial impact at a corporate level | Compromise information asset may lead to medium financial impact at a business vertical level | Compromise information asset may lead to low financial impact at a departmental level | Compromise asset may lead to negligible financial impact at a departmental level |
| **Disruption to Business Operations/ Process(es)** | Compromise to the information asset leading to major and long-term disruption of business at a Corporate level | Compromise to the information asset leading to long-term disruption of business at a Corporate level | Compromise to the information asset leading to mid-term disruption at a Business level | Compromise to the information asset leading to short-term disruption at a departmental level | Compromise to the information asset leading to negligible disruption at a departmental level |
| **Brand Value/ Reputational** | Compromise to information asset may lead to disrepute in the international level | Compromise to information asset may lead to disrepute in the national level | Compromise to information asset may lead to potentially embarrassing, disrepute in the business industry | Compromise to information asset may lead to potentially embarrassing, Internal to the company | Compromise to information asset may lead to potentially embarrassing, Internal to limited group of employees |
| **Legal & Regulatory Compliance** | Compromise to information asset may lead to devastating legal actions at a corporate level leading to conviction, long term consequences, punitive action and high penalties or combination of all four | Compromise to information asset may lead to major legal actions at a corporate level leading to conviction, long term consequences, punitive action and high penalties or combination of all four | Compromise to information asset may lead to legal actions at a business level leading to conviction, medium or short- term consequences, punitive action and penalties or combination of all four | Compromise to information asset may lead to legal actions at a departmental level leading to conviction, medium or short-term consequences, punitive action and penalties. | Compromise to information asset may lead to negligible legal actions at a corporate level leading to conviction, long term consequences, punitive action and high penalties or combination of all four |

| | **Integrity - Safeguarding the accuracy, reliability, readability and completeness of information and processing methods.** | | | | |
|---|---|---|---|---|---|
| **Business impact Parameters** | **Very High (5)** | **High (4)** | **Medium (3)** | **Low (2)** | **Very Low (1)** |
| **Financial Impact** | Modification/deletion of information asset by unauthorized person leading to Very High amount of impact in financial loss. | Modification/deletion of information asset by unauthorized person leading to High amount of impact in financial loss. | Modification/deletion of information asset by unauthorized person leading to Medium amount of impact in financial loss. | Modification/deletion of information asset by unauthorized person leading to Low amount of impact in financial loss. | Modification/deletion of information asset by unauthorized person leading to Very Low amount of impact in financial loss. |
| **Disruption n to Business Operation ns/ Process(es)** | Modification/deletion of information asset by unauthorized person leading to Very High amount of impact in operational loss. | Modification/deletion of information asset by unauthorized person leading to High amount of impact in operational loss. | Modification/deletion of information asset by unauthorized person leading to Medium amount of impact in operational loss. | Modification/deletion of information asset by unauthorized person leading to Low amount of impact in operational loss. | Modification/deletion of information asset by unauthorized person leading to Very Low amount of impact in operational loss. |
| **Brand Value/ Reputational** | Modification/deletion of information asset by unauthorized person leading to Very High amount of impact in reputational and customer loss. | Modification/deletion of information asset by unauthorized person leading to High amount of impact in reputational and customer loss. | Modification/deletion of information asset by unauthorized person leading to Medium amount of impact in reputational and customer loss. | Modification/deletion of information asset by unauthorized person leading to Low amount of impact in reputational and customer loss. | Modification/deletion of information asset by unauthorized person leading to Very Low amount of impact in reputational and customer loss. |
| **Legal & Regulatory Compliance** | Modification/deletion of information asset by unauthorized person leading to Very High amount of impact in legal and regulatory loss. | Modification/deletion of information asset by unauthorized person leading to Very High amount of impact in legal and regulatory loss. | Modification/deletion of information asset by unauthorized person leading to Medium amount of impact in legal and regulatory loss. | Modification/deletion of information asset by unauthorized person leading to Low amount of impact in legal and regulatory loss. | Modification/deletion of information asset by unauthorized person leading to Very Low amount of impact in legal and regulatory loss. |

| | **Availability - Ensuring that authorized users have access to information and associated assets when required.** | | | | |
|---|---|---|---|---|---|
| **Business impact Parameters** | **Very High (5)** | **High (4)** | **Medium (3)** | **Low (2)** | **Very Low (1)** |
| **Financial Impact** | Damage/ malfunctioning to the information asset leading to major and long-term disruption of business at a corporate level causing major financial loss. | Damage/ malfunctioning to the information asset leading to major and long-term disruption of business at a corporate level causing high financial loss. | Damage/ malfunctioning to the information asset leading to major and long-term disruption of business at a corporate level causing medium financial loss. | Damage/ malfunctioning to the information asset leading to major and long-term disruption of business at a corporate level causing low financial loss. | Damage/ malfunctioning to the information asset leading to major and long-term disruption of business at a corporate level causing negligible financial loss. |
| **Disruption to Business Operations/ Process(es)** | Damage/ malfunctioning to the information asset leading to major and long-term disruption of business at a corporate level | Damage/ malfunctioning to the information asset leading to long-term disruption of business at a corporate level | Damage/ malfunctioning to the information asset leading to mid-term disruption at a business level | Damage/ malfunctioning to the information asset leading to short-term disruption at a departmental level | Damage/ malfunction in g to the information asset leading to negligible disruption at a departmental level |
| **Brand Value/ Reputational** | Damage/ malfunctioning to information asset may lead to disrepute in the international level | Damage/ malfunctioning to information asset may lead to disrepute in the national level | Damage/ malfunctioning to information asset may lead to potentially embarrassing, Disrepute in the business industry | Damage/ malfunctioning to information asset may lead to potentially embarrassing, Internal to the company | Damage/ malfunctioning to information asset may lead to potentially embarrassing, Internal to the limited employees |
| **Legal & Regulatory Compliance** | Damage/ malfunctioning to information asset may lead to devastating legal actions at a corporate level leading to conviction, long term consequences, punitive action and high penalties or combination of all four | Damage/ malfunctioning to information asset may lead to major legal actions at a corporate level leading to conviction, long term consequences, punitive action and high penalties or combination of all four | Damage/ malfunctioning to information asset may lead to legal actions at a business level leading to conviction, medium- or short-term consequences, punitive action and penalties or combination of all four | Damage/ malfunctioning to information asset may lead to legal actions at a departmental level leading to conviction, medium- or short-term consequences, punitive action and penalties. | Damage/ malfunctioning to information asset may lead to negligible legal actions at a departmental level not leading to conviction, medium- or short-term consequences, punitive action and penalties. |

## 13. Annexure 3- Criteria for Asset Classification

| Risk Ratings | Very High | High | Medium | Low | Very Low |
|---|---|---|---|---|---|
| SECRET | All or any one business impact criteria is Very High | All 4 and any 3 Business impact criteria is High | Not Applicable | Not Applicable | Not Applicable |
| CONFIDENTIAL | Not Applicable | Any 2 or any 1 business impact criteria is High | All 4 or any 3 business impact criteria is Medium | Not Applicable | Not Applicable |
| INTERNAL | Not Applicable | Not Applicable | Any 2 or any 1 business impact criteria is Medium | All 4 or any 1 business impact criteria is Low | Not Applicable |
| PUBLIC | Not Applicable | Not Applicable | Not Applicable | Not Applicable | All four business impact criteria is Very Low |

This is a Table Representing Asset Classification Result on the sample basis and it's not represent all the possible scenarios

| Financial Impact | Disruption to Business Operations / Process(es) | Brand Value/ Reputational | Legal & Regulatory Compliance | Result |
|---|---|---|---|---|
| **Very High** | Any Value | Any Value | Any Value | Secret |
| Any Value | **Very High** | Any Value | Any Value | Secret |
| Any Value | Any Value | **Very High** | Any Value | Secret |
| Any Value | Any Value | Any Value | **Very High** | Secret |
| **High** | **High** | **High** | Any Value | Secret |
| **High** | **High** | Any Value | **High** | Secret |
| Any Value | **High** | **High** | **High** | Secret |
| **High** | Any Value | Any Value | Any Value | Confidential |
| Any Value | **High** | Any Value | Any Value | Confidential |
| Any Value | Any Value | **High** | Any Value | Confidential |
| Any Value | Any Value | Any Value | **High** | Confidential |
| **Medium** | **Medium** | **Medium** | Any Value | Confidential |
| **Medium** | **Medium** | Any Value | **Medium** | Confidential |
| Any Value | **Medium** | **Medium** | **Medium** | Confidential |
| **Medium** | Any Value | **Medium** | **Medium** | Confidential |
| **Financial Impact** | **Disruption to Business Operations / Process(es)** | **Brand Value/ Reputational** | **Legal & Regulatory Compliance** | **Result** |
| **Medium** | Any Value | Any Value | Any Value | Internal |
| Any Value | **Medium** | Any Value | Any Value | Internal |
| Any Value | Any Value | **Medium** | Any Value | Internal |
| Any Value | Any Value | Any Value | **Medium** | Internal |
| **Low** | Any Value | Any Value | Any Value | Internal |
| Any Value | **Low** | Any Value | Any Value | Internal |
| Any Value | Any Value | **Low** | Any Value | Internal |
| Any Value | Any Value | Any Value | **Low** | Internal |
| **Very Low** | **Very Low** | **Very Low** | **Very Low** | Public |

***Any Value** – It represents the lesser severity value than the mentioned value in the same raw.

## 14. Annexure 4- Severity of Threat Rating

| Severity of Threat Rating | |
|---|---|
| **Rating** | **Description** |
| **5 - Very High** | Threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals |
| **4 - High** | Threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals |
| **3 - Medium** | Threat event could be expected to have limited adverse effect on organizational operations, organizational assets, individuals, other organizations |
| **2 - Low** | Threat event could be expected to have low adverse effect on organizational operations, organizational assets, individuals |
| **1 - Very Low** | Threat event could be expected to have negligible adverse effect on organizational operations, organizational assets, individuals |

## 15. Annexure 5- Likelihood of Occurrence Rating

| Likelihood of Occurrence Rating | |
|---|---|
| **Rating** | **Description** |
| **5 - Very High** | The chance of occurrence of threat due to this vulnerability is very high. Threat can occur frequently. |
| **4 - High** | The chance of occurrence of threat due to this vulnerability is high. Threat can occur frequently, but not so often as of “Very High” |
| **3 - Medium** | The chance of occurrence of threat due to this vulnerability is medium. There is a reasonable probability that this threat shall manifest. |
| **2 - Low** | The chance of occurrence of threat due to this vulnerability is low. |
| **1 - Very Low** | The chance of occurrence of threat due to this vulnerability is negligible. |

## 16. Annexure 6- Risk Impact Rating

| AV = 1 | | Severity of Threat | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| Likelihood of Occurrence of Threat | 1 | 1 | 2 | 3 | 4 | 5 |
| | 2 | 2 | 4 | 6 | 8 | 10 |
| | 3 | 3 | 6 | 9 | 12 | 15 |
| | 4 | 4 | 8 | 12 | 16 | 20 |
| | 5 | 5 | 10 | 15 | 20 | 25 |

| AV = 2 | | Severity of Threat | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| Likelihood of Occurrence of Threat | 1 | 2 | 4 | 6 | 8 | 10 |
| | 2 | 4 | 8 | 12 | 16 | 20 |
| | 3 | 6 | 12 | 18 | 24 | 30 |
| | 4 | 8 | 16 | 24 | 32 | 40 |
| | 5 | 10 | 20 | 30 | 40 | 50 |

| AV = 3 | | Severity of Threat | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| Likelihood of Occurrence of Threat | 1 | 3 | 6 | 9 | 12 | 15 |
| | 2 | 6 | 12 | 18 | 24 | 30 |
| | 3 | 9 | 18 | 27 | 36 | 45 |
| | 4 | 12 | 24 | 36 | 48 | 60 |
| | 5 | 15 | 30 | 45 | 60 | 75 |

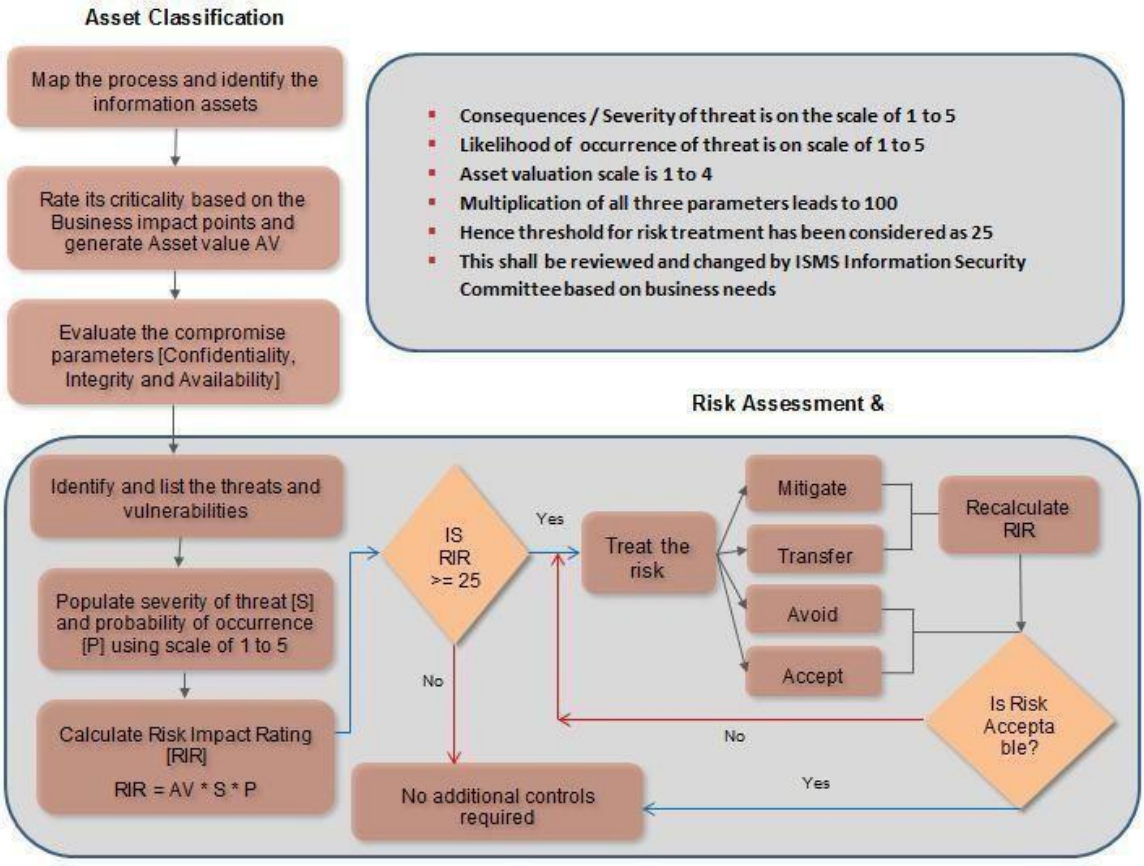
| AV = 4 | | Severity of Threat | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| Likelihood of Occurrence of Threat | 1 | 4 | 8 | 12 | 16 | 20 |
| | 2 | 8 | 16 | 24 | 32 | 40 |
| | 3 | 12 | 24 | 36 | 48 | 60 |
| | 4 | 16 | 32 | 48 | 64 | 80 |
| | 5 | 20 | 40 | 60 | 80 | 100 |

**Legends**

| | |
|---|---|
| | Control to be applied |
| | No Control Required |

## 17. Annexure 7- Risk Mitigation

Based on the risk treatment option selected, the Information Security team shall identify controls that need to be implemented to treat the risk.



## 18. Annexure 8- Terms and definition.

18.1. **Asset:** Asset is any entity / object or resource that are valuable for the organization or is necessary for the business Operation, Asset need to protect from the potential threats or risk.

18.2. **Threat:** Threat is defined as any potential event or circumstance that can cause harm to an organization's assets.

18.3. **Risk:** a risk refers to the potential occurrence of an event or circumstance that could have a negative impact on an organization's information security objectives. This impact may involve threats exploiting vulnerabilities in information assets, leading to potential harm such as unauthorized access, disclosure, alteration, or destruction of information. Risks can stem from various sources, including internal and external factors, human error, technological vulnerabilities, and environmental hazards.

18.4. **Risk Assessment:** Risk assessment is a systematic process of identifying, analyzing, evaluating, and prioritizing risks to an organization's assets, including information, people, processes, and technology.

18.5. **Risk Treatment**: Risk treatment is the process of selecting and implementing measures to modify, mitigate, transfer, or accept identified risks.