SUNRISE GILTS & SECURITIES PRIVATE LIMITED

IT THREAT – RISK ASSESSMENT POLICY

(EFFECTIVE DATE: 10/06/2025)

SUNRISE GILTS & SECURITIES PVT. LTD.
AHMEDABAD

Author:	PRATIK KUMAR MORE
Owner:	PRATIK KUMAR MORE
Approved by:	BOARD OF DIRECTORS
Organization:	SUNRISE GILTS & SECURITIES PRIVATE LIMITED
Version No:	1.1
Approval Date	28/05/2025
Effective Date:	10/06/2025

Document Control

Document Title **IT Threat-Risk Assessment Policy**

Version History

Version No.	Version Date	Author	Summary of Changes
1.0	13/06/2019	PRATIK KUMAR MORE	NA
1.1	10/06/2025	PRATIK KUMAR MORE	Review and Approval of BOD

Approvals

Name	Title	Approval Date	Version No
PRATIK KUMAR MORE	IT Threat-Risk Assessment Policy	13/06/2019	1.0
PRATIK KUMAR MORE	IT Threat-Risk Assessment Policy	28/05/2025	1.1

SUNRISE GILTS & SECURITIES PVT. LTD.
AHMEDABAD

3. IT THREAT-RISK ASSESSMENT POLICY

1.1 PURPOSE

All information assets need not be equally important for SUNRISE GILTS & SECURITIES PRIVATE LIMITED's operations for achieving its vision and mission. Some assets are more important and need close attention and enhanced level of protection to ensure that mission critical systems are on and functioning.

The primary purpose of risk management is to make judicious use of the resources and provide the best possible protection at an acceptable cost. Information Risk Assessment consists of under noted components:

- Risk profiling - Identification of risk on the backdrop of perceived threats to information asset and vulnerability associated with information asset
- Assessing the risk
- Selecting the most effective controls to reduce the risk to an acceptable level

1.2 SCOPE

This policy applies to:

- All the company assets like IT infrastructure, Information stored in the organization.
- All staff (permanent & on contractual basis) and non-employees (contractors, consultants, suppliers, vendors etc.)

1.3 POLICY STATEMENTS

1.3.1 PROCESS

Information Risk Assessment Framework is a sequence of steps used to identify, understand and mitigate the risks to the confidentiality, integrity and availability of organisation information to the acceptable level.

SUNRISE GILTS & SECURITIES PVT. LTD. ★ AHMEDABAD

A risk assessment is a pre-requisite to the formation of mitigation strategies, and this guides the organisation as it develops, implements, tests, and maintains its information systems security posture. This is an ongoing part of the information security management program.

1.3.2 ASSET & RISK MANAGEMET METHODOLOGY

The initial asset inventory & risk assessment and reviews are performed by the Asset Owner in consultation with Technology Officer. Risk assessment is reviewed once in every twelve months.

Further, risk assessment is also performed in the following circumstances,

- When new systems are implemented, or applications are developed or acquired.
- When critical business processes & procedures are changed & which may impact on information security.
- When major changes are made to IT infrastructure.

<u>Methodology:</u>

The Risk Assessment Methodology defines the methodology used by SUNRISE GILTS & SECURITIES PRIVATE LIMITED to assess risks to the confidentiality, integrity and availability of information assets. The risk assessment needs to be carried out for important assets identified by the asset management processes and functions in SUNRISE GILTS & SECURITIES PRIVATE LIMITED.

<u>The Risk Assessment Evaluation:</u>

- Consider IT Asset Classification from IT Asset Management Policy to identify valuation of IT Assets.
- Identified threats and vulnerabilities for a particular asset group are evaluated independent of existing controls.
- Control strengths that SUNRISE GILTS & SECURITIES PRIVATE LIMITED already has in place are then mapped to evaluate the risks.

SUNRISE GILTS & SECURITIES PVT. LTD.
AHMEDABAD

- On completing the Risk Assessment, each asset group will have multiple risk values based on threat/vulnerability pairs mapped to existing control strengths.
- Necessary controls are used towards a Risk Treatment plan.
- Any residual risks above baseline levels after Risk Treatment need to be formally accepted by the SUNRISE GILTS & SECURITIES PRIVATE LIMITEDsenior management.

1.4 IDENTIFICATION & VALUATION OF ASSETS

1.4.1 ASSET IDENTIFICATION

Assets encompass all those items which contribute to the provision of information required by SUNRISE GILTS & SECURITIES PRIVATE LIMITED to conduct its business. An asset may be a component or part of a total system to which SUNRISE GILTS & SECURITIES PRIVATE LIMITED will assign a value and arrange for protection according to value. Following are the various categories of assets accordance with asset management process.

- All IT assets shall be identified by SUNRISE GILTS & SECURITIES PRIVATE LIMITED and an asset inventory shall be maintained by IT Security.
- IT assets shall be organized under categories mentioned in IT Asset Management policy.
- All IT assets shall be mapped with specific owners at different level of management in SUNRISE GILTS & SECURITIES PRIVATE LIMITED.
- IT Assets can be grouped for conducting IT risk assessments. It may not be practical or useful to perform IT risk assessment for individual assets in all cases.
- IT risk assessment shall attempt to optimize effort by using a combination of baseline approach for asset groups and detailed IT risk analysis for critical assets.
- Grouping of assets for the purpose of IT risk assessment shall use the following criteria:
    - Grouped assets shall have the same asset value in terms of criticality and sensitivity
    - Grouped assets shall have similar threat profiles. This means that similar threats, vulnerabilities and controls are applicable
    - The overall functionality of the grouped assets is similar
    - Grouped assets shall belong to same asset owners.

<u>The asset valuation methodology is as below:</u>

The value of an asset is based on the impact to SUNRISE GILTS & SECURITIES PRIVATE LIMITEDif the asset suffers from loss of confidentiality, integrity, or availability. Six dimensions shall be considered to evaluate the potential impact on SUNRISE GILTS & SECURITIES PRIVATE LIMITED, and thus derive the value of the asset:

- Customers affected
- Critical systems affected
- Financial loss
- Brand and reputation
- Proprietary information
- Regulatory implication

For each asset, "What is the extent of damage along these six dimensions if the asset is compromised in Confidentiality, Integrity, or Availability?" is to be determined.

1.4.2 ASSET CLASSIFICATION

- All IT assets of SUNRISE GILTS & SECURITIES PRIVATE LIMITED shall be classified by the Asset Owners as per Asset Management Policy based on their sensitivity and impact to business operations. SUNRISE GILTS & SECURITIES PRIVATE LIMITED classifies assets as one of the following:
  - High – impact that may stall the business
  - Medium – impact that may affect the business
  - Low – impact that has no significant effect on the business
- All assets of SUNRISE GILTS & SECURITIES PRIVATE LIMITED shall be valued by the Asset Owners based on the business impact on the loss of Confidentiality (C), Integrity (I) and Availability (A) in terms of High, Medium and Low.
  - Confidentiality – business impact as a result of disclosure of the asset
  - Integrity – business impact as a result of modification of the asset
  - Availability – business impact as a result of failure of the asset
- The designated asset owner shall review and revise the classification given to an asset based on changes in business requirements.
- Asset register for IT risk assessment along with valuation shall be maintained by the Technology Officer.

SUNRISE GILTS & SECURITIES PVT. LTD.
AHMEDABAD

1.4.3 LIKELIHOOD OR PROBABLITY OF THREAT OCCURANCE

While determining the probability, the threat frequency in terms of how often it might occur, based on experience and statistics shall be considered. The likelihood of threat occurrence is valued using the following scale.

Unlikely	=	1
Could happen	=	2
Very Likely	=	3

1.4.4 IMPACT OF THE THREAT ON CIA OF THE ASSET GROUP

Once the likelihood of threats is valued, identify the affected aspect (C, I and A) and assess the impact on the asset if the threat were to materialize. Impact of threat on asset (CIA) is valued using the following scale:

Low	=	1
Medium	=	2
High	=	3
Very High	=	4

1.4.5 IDENTIFICATION & VALUATION OF VULNERABILITIES

Vulnerabilities are weaknesses associated with an organization's assets. These weaknesses may be exploited by a threat causing unwanted incidents that may result in loss, damage or harm to these assets.

The vulnerability identification should identify the weaknesses related to the assets by considering the following:

SUNRISE GILTS & SECURITIES PVT. LTD.
AHMEDABAD

- Physical environment
- Personnel and administration procedures and controls
- Hardware, software or communication equipment and facilities

Vulnerabilities are categorized into Low (1), Medium (2), High (3), and Very High (4) based on the levels of vulnerability in the assets

- Low - The possibility of the vulnerability being exploited is very less
- Medium - The vulnerability might be exploited
- High - The vulnerability can be easily exploited
- Very High - The vulnerability can be very easily exploited

1.4.6 IDENTIFICATION & VALUATION OF CONTROL STRENGTH

After identification and valuation of threats and vulnerabilities, the existing processes and control in the SUNRISE GILTS & SECURITIES PRIVATE LIMITED environment to minimize the threat and vulnerabilities are identified. For each control, a control strength value is calculated. The "Control Strength" is calculated from "Nature of Control" and "Type of Implementation".

A numerical value is assigned to the Type of Implementation:

Manual	=	1
Automated	=	2

A numerical value is assigned to the Nature of Control:

Awareness	=	1
Recovery	=	2
Detection/Deterrent	=	3
Preventive	=	4

The control strength value is calculated using the following formula:

Control Strength = Type of Implementation x Nature of Control

If there is more than one control; all control strengths are added to arrive at the final strength.

1.4.7 CALCULATION OF RISK VALUES & IDENTIFYING RISK OWNER

All the threats and vulnerabilities a particular asset may be exposed are identified and the existing controls are implemented in the organization are listed and the control strengths are calculated.

The Risk Score is calculated using the following formula:

Risk Score = Asset Value x Threat Value x Vulnerability Value

The Risk Value is calculated using the following formulas based on the existing controls availability:

- Risk Value = Risk Score / Control strength - If existing controls are available.
- Risk Value = Risk Score / (1 + Control strength) - If there are no existing controls.

Risk Ownership

Overall ownership of risk shall remain with Asset owners shall,

- Assume ownership of risk pertaining to their asset.
- Be accountable to ensure that appropriate controls, commensurate with the security classification level are maintained and the risks associated with the assets are managed.

1.4.8 INITIAL BASE LEVEL FOR ACCEPTABLE RISK VALUES & PRIORITIZATION OF RISK

Risk Treatment requires a baseline for prioritizing and treating risks. The baseline level indicates the acceptable values of risk. Risk values within the baseline level may be accepted. Risk values above this level require treatment based on the priority.

SUNRISE GILTS & SECURITIES P. LTD. ★ AHMEDABAD

Risk values above baseline should be prioritized for risk treatment based on the subjective analysis of risk values, risk exposure, likelihood of occurrence, and likelihood of detection, severity of impact and resource requirements.

Priority of risk would be defined as following:

Threat Value		Low				Medium				High				Very High			
Vulnerability Value		L	M	H	VH	L	M	H	VH	L	M	H	VH	L	M	H	VH
Asset Value	Low	1	2	3	4	2	4	6	8	3	6	9	12	4	8	12	16
	Medium	2	4	6	8	4	8	12	16	6	12	18	24	8	16	24	32
	High	3	6	9	12	6	12	18	24	9	18	27	36	12	24	36	48
	Very High	4	8	12	16	8	16	24	32	12	24	36	48	16	32	48	64

Some risk values may remain above this baseline level because they cannot be immediately treated due to various factors such as lack of resources, mitigation cost exceeds benefit, etc. These need to be separately accepted at their higher risk values and signed off by the Technology Officer.

Management reviews the acceptable risk values based on available resources and budget for risk treatment. The Technology Officer has formally accepted an initial SUNRISE GILTS & SECURITIES PRIVATE LIMITED- baseline level=8.

1	2	3	4	6	8	9	12	16	18	24	27	32	36	48	64
Acceptable Risks						Non-Acceptable Risks									

The above shows the 8 as the baseline level. Risk values above this level are by default non-acceptable unless formally accepted by management.

Justification for choosing a Baseline level of 8

SUNRISE GILTS & SECURITIES PVT. LTD. ★ AHMEDABAD

To calculate the baseline value:

- The maximum risk score is 64.
- An acceptable baseline level of 10% would ensure that 90% of the identified risks are put on a treatment plan.
- Thus, the baseline level of 8 is chosen above which the risks shall be treated, and exceptions need to be formally signed off.
- The Technology Officer may decide to further decrease the baseline level in subsequent management reviews.

1.4.9 RISK TREATMENT / RISK ACCEPTANCE

Risk Treatment requires a baseline for prioritizing and treating risks. Risk values within the baseline level may be accepted. Risk Assessment Risk Treatment would be conducted annually. It would be schedule and informed to the key stakeholders one week prior to the start date.

It is seldom possible to eliminate risks to information in terms of confidentiality, integrity, or availability. Identification of the appropriate security controls as per the ISO27001 is necessary before the implementation.

- Any of the following IT risk treatment strategies or a suitable combination can be adopted to mitigate the IT risk:
    - Transfer Risk
    - Tolerate (Accept) Risk
    - Treat the Risk
    - Terminate the Risk

When evaluating the levels of acceptable risk in managing a specific risk, the Technology Officer should consider the following issues:

- Location – The location determines the probable risks from accidental damage, e.g. from fire, contamination or floods.
- Existing Security – Physical, logical and personnel security measures already in place.
- Awareness on information security across organization.

SUNRISE GILTS & SECURITIES PVT. LTD.
AHMEDABAD

- Number of security weaknesses – The higher the number of security weaknesses, the higher the risk of exposure/penetration.
- Facilities available – The more sophisticated the facilities available to a malicious user, the higher are the probability of exploiting the security weaknesses.
- Business continuity planning – The ability of existing business continuity measures to deal with an event.

The risks are managed to the level of acceptable risk through policies that avoid the risk, transfer the risk, reduce the vulnerabilities, reduce the threats, reduce the possible impacts, detect unwanted events, or employ a combination of the above.

Where action is required to manage a risk, the management decisions are documented in the management team meeting minutes and communicated to the appropriate member(s) of staff for implementation of the control/countermeasure. Such decisions may require a new policy statement or the amendment of an existing policy.

Where a risk is identified, but controls/countermeasures is not implemented because of financial, environmental, technological, cultural, time-scale or other reasons, then risk is accepted and business exception is taken for the same. These points should be reviewed on a regular basis to ensure the decision remains valid.

Management reviews of the Risk Management shall periodically review the acceptable risk values based on available resources and budget for risk treatment.

1.4.10 MONITORING AND REVIEW

- Having identified the risks and determined a plan of remedial action, it is essential that assurance regarding the effectiveness of the action is obtained.
- All responsible risk owners will provide periodical updates, to the Technology Officer regarding the progress made in reducing/removing risks. This information will be used to update the Risk Register.

1.4.11 RESPONSIBILITIES

SUNRISE GILTS & SECURITIES PVT. LTD. ★ AHMEDABAD

The responsibility for the upkeep of the asset identification and perceived valuation remains with the Technology Officer who review the situation regularly, and especially when any significant changes are made to the departments.

Changes in SUNRISE GILTS & SECURITIES PRIVATE LIMITED organizational structure may result in changes to process ownership. Handover of responsibilities includes acceptance of the risk assessment procedure and understanding of the risk in the process or function.

The new and emerging risk will be identified in the following manner:

1. Based on inputs and feedback obtained by the Technology Officer from the process personnel or through other means
2. During the internal or external audits
3. Based on inputs from the management

The identified risks need to be added to the risk assessment sheet.

1.4.12 RESIDUAL RISK APPROVAL & TREATMENT PROCESS

Identified risks from the Risk Assessment should be extracted and condensed to form a unique list of residual risks that when addressed would bring down the risk levels to acceptable values.

The minutes of the meeting should be recorded to serve as evidence for management approval and acceptance of the proposed treatment activities. The Residual Risk Tracker should serve as a dynamic document that details treatment items for all current risks above acceptable baseline levels and their status updates.

SUNRISE GILTS & SECURITIES PVT. LTD.
AHMEDABAD