RISK MANAGEMENT POLICY

DOCUMENT CONTROL PAGE

Document ID	SCG/RMF/015/1.0
Security Classification	Confidential
Date Issued	23-June-2025
Version	1.0
Project Name	NA
Author	AJ KHAN

VERSION HISTORY / CHANGE HISTORY

Version	Date Issued	Issued to	Comments
0.1	23-June-2025		Issued for internal review
1.0	23-June-2025		Final version

REVIEWERS

Version	Review Date	Reviewed By	Comments
0.1	23-June-2025		Issued for internal review
1.0	23-June-2025		Final version

APPROVERS

Version	Date Approved	Approved By	Comments
0.1	23-June-2025		Issued for internal review
1.0	23-June-2025		Final version

DISTRIBUTION LIST

Date	Name / Distribution List	Comments
23-June-2025	Customer_DL_ABC	Published to Customer ABC

DOCUMENT CONTROL PAGE

RELATED DOCUMENTS

DOC_ID	DOC Version#	DOC Link	Comments
SCG/BASEINS/005/1.0			Base Template Instructions
SCG/PXF/008/1.0			Policy Exception Form
SCG/RXT/037/1.0			Risk Exception Template

CONFIDENTIALITY STATEMENT

This document is the exclusive property of [SecureCyberGates]. This document contains proprietary and confidential information. Duplication, Redistribution, or use, in whole or in part, in any form, requires consent of [SecureCyberGates].

[SecureCyberGates] may share this document with auditors under non-disclosure agreements [NDA] to demonstrate Security Audit requirement compliance.

Contents

1) Objective 6

2) Roles &Responsibilities 6

3) Scope 6

4) Risk management Process 7

4.1) Objective 7

4.2) Standard 7

4.3) Guidelines 7

4.4) Procedures 7

4.4.1) Risk Management Flow 8

4.4.2) Risk Communication and Consultation Flow 13

5) Employee Training and Awareness 14

6) Compliance and Monitoring 14

7) Escalation Matrix 14

8) Policy Exceptions 15

9) Policy Review and Updates 15

10) Conclusion 16

1) Objective

Our Risk Management Policy serves as guidance for ensuring that information security-related risk is visible to and understood by the business unit(s) that own the assets and / or processes involved. Since the information security team merely facilitates and educates the management of risk, business units and other key stakeholders are expected to be active participants in [SecureCyberGates]'s risk discussions.

This Risk Management Policy establishes the standards that promote fairness in the management of risk at the appropriate level of corporate management which is of critical importance to [SecureCyberGates]'s long-term success. Therefore, [SecureCyberGates] shall periodically assess the risk to operations, assets and data that are associated with the processing, storage, or transmission of information to support [SecureCyberGates]'s business processes and take appropriate action to remediate unacceptable risks.

2) Roles &Responsibilities

Roles	Responsibilities
CISO	Accountable - Overseeing the implementation and enforcement of this policy [Review and Approve Risk Management Policy]
IT/Security Team	1. Responsible for ensuring Risk Management requirements are in place 2. Responsible for enforcing these Risk Management requirements
BU Heads or Project Managers	Ensuring that employees under their supervision comply with this policy. [Review and Approve Risk Management Policy]
Employees / Contractors	1. Read this Risk Management Policy 2. Ask questions /Provide Feedbacks 3. Report possible or actual violations of this Policy.

3) Scope

This Policy applies to anyone who conducts business for or on behalf of [SecureCyberGates] including:

- All employees
- Management and company owners
- External business partners who act on [SecureCyberGates]'s behalf or in our interest as Third Party Representatives

It is important to note that every situation may not be addressed in this Risk Management Policy; if you are unsure how [SecureCyberGates] standards or values apply in a given situation, please ask questions and seek further guidance from the Security team.

Each and every one of us are responsible for ensuring that we follow these guidelines, and we will be held accountable for upholding our commitments to this Risk Management Policy.

This Policy document defines Risk management Process for information security related Risks , Real time Risk details are not available in this Policy document.

4) Risk management Process

4.1) Objective

The organization develops, implements, and governs processes and documentation to facilitate the implementation of an enterprise-wide Information Security risk management policy, as well as associated standards, controls, and procedures.

4.2) Standard

[SecureCyberGates] is required to develop and implement an enterprise-wide information security risk management strategy that includes:

1. A formal risk assessment that is performed **at least annually** and **upon significant changes** to the corporate environment (e.g., acquisition, merger, relocation);
2. Identification of critical assets, current safeguards, effectiveness of safeguards, threats, and vulnerabilities;
3. A review of all processes involving creating, receiving, maintaining, and transmitting of sensitive data; and
4. Assigning responsibility to validate security controls.

4.3) Guidelines

[SecureCyberGates]'s information security-specific risk management strategy should include an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance and approaches for monitoring risk over time.

4.4) Procedures

Control Activity: In house Security and IT team:

1) Uses vendor-recommended settings and industry-recognized secure practices to ensure controls are sufficient for managing risk that includes:

A formal Risk Management Program that includes:

- An unambiguous expression of the risk tolerance;
- Acceptable risk assessment methodologies; and
- Risk mitigation strategies.

A process for consistently evaluating and monitoring risk over time;
A process for conducting risk assessments annually and upon significant changes to the corporate environment (e.g., acquisition, merger, relocation);
Identification of:

- Critical assets
- Current safeguards; and
- Effectiveness of safeguards, threats, and vulnerabilities.

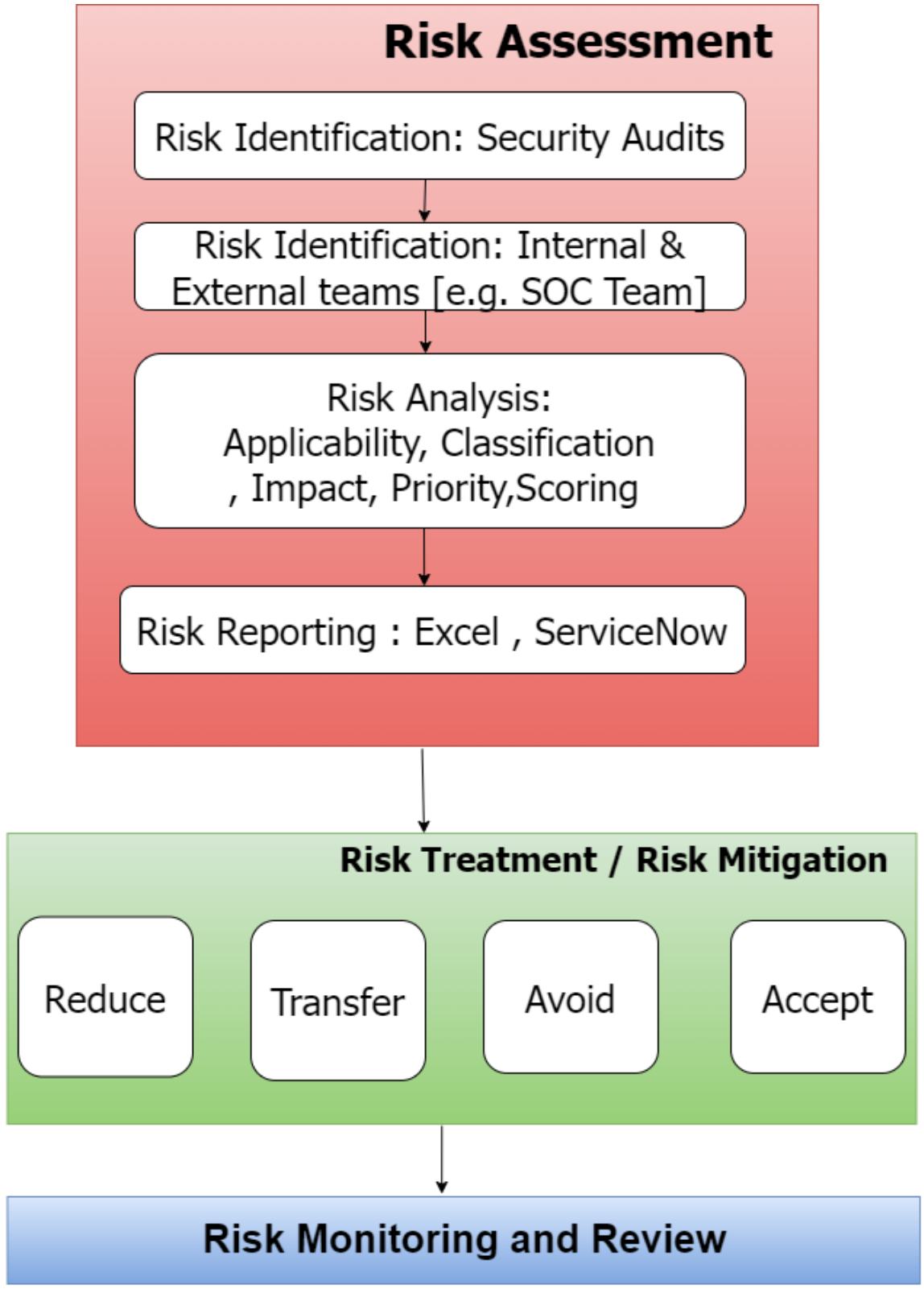
Reviewing processes involving creating, receiving, maintaining, and transmitting of sensitive data; and
Assigning responsibility to validate security controls.

2) On at least an annual basis, during the 1st quarter of the calendar year, reviews the process for non-conforming instances. As needed, revise processes to address necessary changes and evolving conditions. Whenever the process is updated:
   Distributes copies of the change to key personnel; and
   Communicates the changes and updates to key personnel.
3) If necessary, requests corrective action to address identified deficiencies.
4) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
5) If necessary, document the results of corrective action and note findings.
6) If necessary, requests additional corrective action to address un-remediated deficiencies.

4.4.1) Risk Management Flow

Risk Management at [SecureCyberGates] is divided in 5 Phases

#	Phase	Description
1	Risk Identification	This section will describe various system from where risks are identified.
2	Risk Analysis	This section will describe detail analysis done for identified risk.
3	Risk Reporting	Document Risk details and store it centrally.
4	Risk Treatment / Risk Mitigation	Once Risk is applicable, this section will determine how we can mitigate that risk.
5	Risk Monitoring and review	This section will describe how risks are reviewed & monitored [After Mitigation] e.g., Residual Risks



5

Information Security Risk management Process

Phase 1 - Risk Identification

Risks are identified from various sources in [SecureCyberGates].
Security Audits: Security Audits conducted by Internal and External teams / vendors. These Audits include inspection of Infrastructure [Server, Network, Database, and Application], Vulnerability Assessment and Penetration Testing done on Web applications, Mobile applications by internal teams and external/3rd Party teams. Source code reviews and Software Composition analysis. Another source of Risks identifications are Internal and external teams from various department of [SecureCyberGates] [e.g. IT Team , SOC [Security Operations center team] , Project team , Support team] may identify Risk during Project Execution, Change Request etc.

Phase 2 - Risk Analysis

Risk Analysis involves investigating in more details which include below items:

Item	Description
Risk Applicability	Determine Whether risk is applicable or not to [SecureCyberGates]. If Risk is Not applicable then document the risk as NA with proper justification approved by management.
Risk Classification	Classify the Risk as per category and Attack type.
Risk Impact [Severity]	Negligible, Minor, Medium, High, Critical.
Risk Priority	Priority would be from P1 to P4 [P1 -> Critical P2-> High, P3-> Medium, P4->Low]
Risk Likelihood	How likely this risk can occur in real world? [1 -> Very Rare, 2->Rare, 3-> Possible, 4-> Likely, 5-> Very Likely]
Department	Assign this Risk to [SecureCyberGate] Department [Risk Owner can be a dedicated person from that department]

Phase 3 - Risk Reporting

Risk details should be documented under central tool like ServiceNow, RSA Archer or simple excel sheet. Backups of Risk Should be taken on Weekly basis in case any application is NOT available. ONLY authorized individuals should be provided access to information secruity risks. This would be our Central Risk Register.
e.g. of some tool below:

Phase 4- Risk Treatment / Risk Mitigation

After Risk analysis is done, security team [along with other teams] will decide to **accept** this risk, **avoid** it, **transfer** it or to **Reduce** it by putting some Security controls or requirements.

Reduce / Mitigate: Reduce/Mitigate the risk impact by putting security controls in place. Risk can be fully mitigated or the likelihood of the risk is reduced. When a risk is reduced, a strategy is implemented to remediate the risk to an acceptable level.

Risk reduction can be achieved through management controls or other arrangements which reduce the frequency of, or opportunity for, error– such as alternative procedures, quality assurance, testing, training, education, supervision, review, documented policy, and procedures.

Examples of reducing risk include, but are not limited to:

- Apply compensating controls.
- Remediate vulnerabilities to correct identified deficiencies.

Transfer: Transfer the risk to a 3rd party [If it does not belong to [SecureCyberGates], we transfer it to respective Clients / Other vendors]

When risk is transferred, a strategy is implemented that shares or transfers the risk away from [SecureCyberGates].

Risk can be transferred by shifting the responsibility for a risk to another party. Risks may be transferred in **full, or they may be shared** with another party. Risks should be allocated to the party that can exercise the most effective control over those risks.

Examples of transferring risk include, but are not limited to:

- Purchase additional **information security insurance.**
- Select a vendor that will accept indemnification for the risk associated with providing the service

Avoid: Eliminate the risk by not taking any action that would mean the risk could occur. Develop an alternative strategy where this risk cannot occur. Adopt different technical solutions, change project scope, and modify project plans.

When a risk is avoided, a decision is made not to proceed with the activity.

Wherever possible, risk avoidance measures should be designed to be embedded in normal business processes, activities, and systems. Those measures should not impede the logical or natural flow of existing processes and should be easy to understand and appreciate.

Examples of avoiding risk include, but are not limited to:

- Terminate the project.

- Select a different solution that does not have the same risk.

Accept: Accept the risk, but due to some other issues [e.g., Time consuming, Costly to Mitigate, etc.] we don't Mitigate that risk. A risk is **accepted with no action taken** to mitigate that Risk. Approval is required by management for this. Kindly find Risk exception template **Document ID: SCG/RXT/037/1.0**

While accepting risk is an option for management, the decision needs to be reasonably justified and documented.

Examples of reducing risk include, but are not limited to:

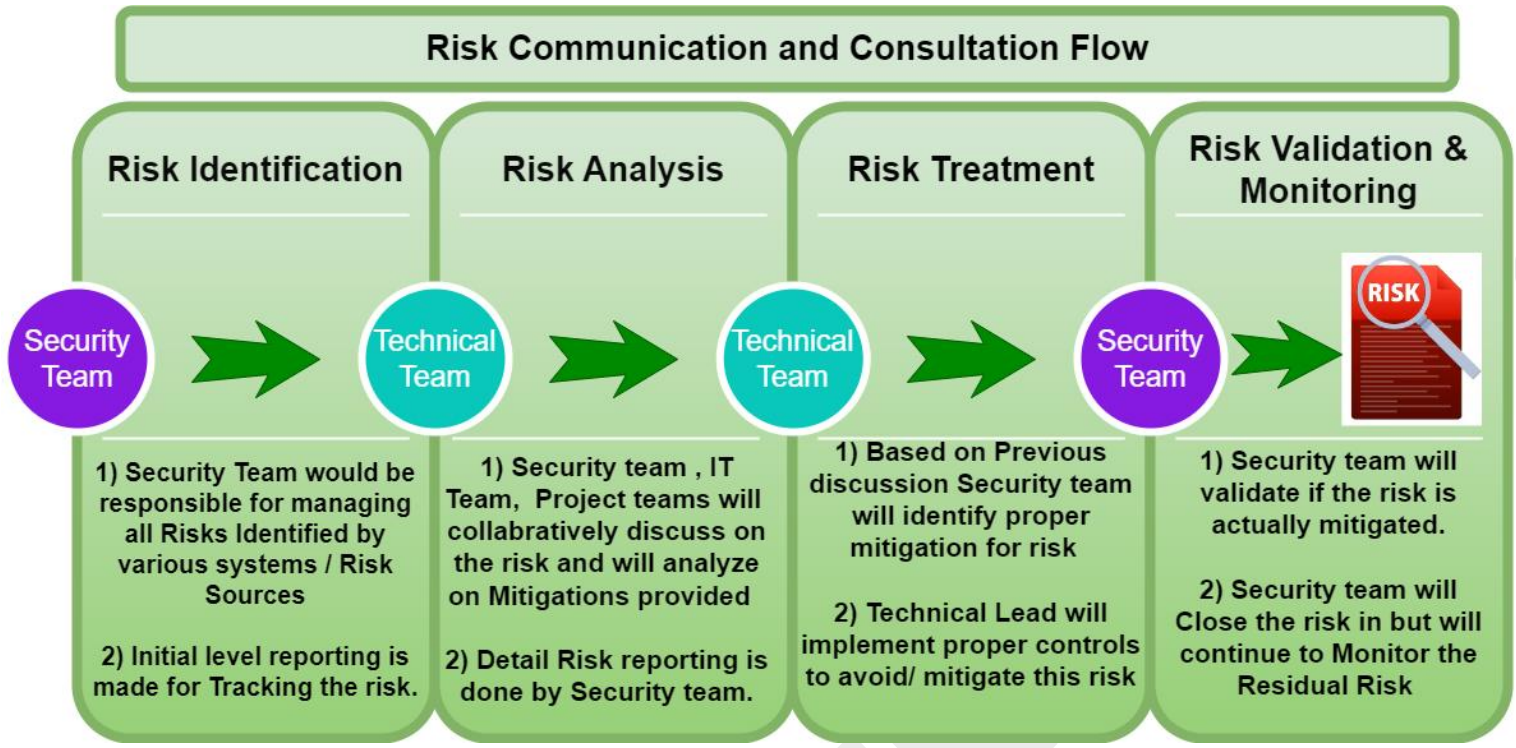
- Continue with the project, being fully aware of the risks.
- Choosing not to remediate vulnerabilities, based on untenable remediation costs.

Accepting and retaining the risk is the least desirable option for [SecureCyberGates]. However, after careful analysis of the cost of risk treatments, management may determine that risk cannot be avoided, reduced, or transferred, or where the cost to do so is not justified (usually, because the likelihood and consequences are low). These retained risks should be monitored, and it must always be remembered that al unidentified risks are retained risks.

Phase 5- Risk Monitoring and Review

Review and monitor the risk periodically [Update the risk register periodically]. Take all applicable risks review during monthly Security meetings. Security team will validate if risk is mitigated before closing the risk. Provide

4.4.2) Risk Communication and Consultation Flow



5) Employee Training and Awareness

5.1) All [SecureCyberGates] employees SHOULD undergo training and assessment on this policy during their initial induction [Onboarding].

5.2) Security team to conduct periodic trainings **ATLEAST ONCE** a year.

6) Compliance and Monitoring

6.1) Compliance with this policy is **MANDATORY**. Employees violating this policy will be subject to disciplinary action up to and including termination.

6.2) Third-party users, contractors, and vendors who **FAIL** to comply with this policy may have their access to [SecureCyberGates]systems , Application and networks revoked or suspended until compliance is achieved. Repeated or severe violations may result in the termination of their contracts or business relationships with [SecureCyberGates].

6.3) Periodic Audits and Assessments : [SecureCyberGates]'s IT department, in collaboration with the Information Security team, will conduct periodic audits and assessments to evaluate compliance with this policy.

7) Escalation Matrix

7.1) In case of any policy violations issues, the following escalation structure shall be followed to ensure timely resolution and appropriate accountability:

Level	Role	Contact
Level 1	Team Lead /Reporting Manager	First-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]
Level 2	Group Manager / Senior Managers	Second-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]
Level 3	CISO	Final-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]

7.2) Employee SHOULD provide sufficient evidences and details , Clear description of the issue.

7.3) Security team to define issue severity and proper SLA for issue resolution as per severity.

8) Policy Exceptions

8.1) There may be requirements where Employee needs policy exception for legitimate reasons, In such cases, employee should follow POLICY EXCEPTIONS template and approval process. **[Kindly refer Policy exception form [Document ID SCG/PXF/008/1.0]]**

9) Policy Review and Updates

9.1) This policy shall be periodically reviewed **[Atleast Once in a YEAR]**and updated to ensure its effectiveness, relevance, and alignment with [SecureCyberGates]objectives,legal requirements and industry best practices.

9.2) Feedback from employees, stakeholders, and external audits shall be solicited and considered for continuous improvement of the policy and associated procedures.

9.3) Regular audits and inspections shall be conducted to assess compliance with this policy and associated procedures, with non-conformances addressed through corrective actions and preventive measures.

9.4) Any updates or revisions to this policy will be communicated to all employees and relevant stakeholders through appropriate channels. Employees are responsible for familiarizing themselves with the latest version of the policy and adhering to its requirements.

10) Conclusion

By implementing and adhering to this comprehensive Risk Management policy, [SecureCyberGates]aims to protect its sensitive information, intellectual property, and critical systems from unauthorized access and data breaches. This policy aligns with industry best practices and incorporates robust requirements for risk management, and system development standards.

SECURE CYBER GATES

THANKYOU!
FOR CYBER-SECURITY RELATED UPDATES, KINDLY FOLLOW BELOW PAGES...

https://www.linkedin.com/in/aj57/
https://www.linkedin.com/company/securecybergates
https://securecybergates.com/services
https://www.youtube.com/@SecureCyberGates
https://hackerone.com/crypto-khan
https://x.com/securecybergate
securecybergates@gmail.com

SECURE CYBER GATES