Information Systems and Technology Security

Risk Management Policy & Procedure

Original author's name:	Pkkirisankar Jagannath
Most recent date:	November 22, 2022
Most recent version number:	v1.0
Process owner:	Program Director

Document History

Version	Date	Revised by	Description
v1.0	November 22, 2022	Pkkirisankar Jagannath	Original Draft
v1.0	November 22, 2022	Kulpreet Singh	Ratified Version

Designated document recertification cycle in days:	[Cycle 30 90 180 **365**]
Next document recertification date:	November 22, 2023

Risk Management Policy & Procedure

The **22nd Century Technologies** (the "Company") **Risk Management Policy & Procedure** defines objectives for establishing specific standards for protecting the confidentiality, integrity, and availability of Company information assets.

This Risk Management Policy & Procedure builds on the objectives established in the **Asset Protection Standard** and the **Auditing Standard.** It provides specific instructions and requirements for managing information assets and risks to the organization. These instructions address risk assessment and management requirements for printed, electronically stored, and electronically transmitted information.

The protection of Company, Client and Consumer information is paramount. Negligence in adhering to these standards has significant implications in both domestic and international laws or regulations that may result in legal or administrative actions against the individual and the company.

1. Scope

All activities undertaken by the Company carry an element of risk. The exposure to these risks is managed through the practice of Risk Management. In managing risk, it is the Company's practice to take advantage of potential opportunities while managing potential adverse effects. Managing risk is the responsibility of everyone in the Company.

This policy outlines the Company's risk management process and sets out the responsibilities of the Board, the Audit and Risk Committee, the CEO, the CEO, senior management and others within the Company in relation to risk management.

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company premises or who have been granted access to Company information or systems, are covered by this standard and must comply with associated guidelines and procedures.

- **Confidentiality classifications** are defined in the Information Classification Standard.

- **Information assets** are defined in the Asset Identification and Classification Policy.

Risks have been described in terms of combination of the consequences of an event occurring and its likelihood of occurring.

Risk is the chance of something happening that will have an impact on objectives and risk management can be described as the culture, processes and structures that are directed towards realizing potential opportunities whilst managing an adverse effect.

The Company's risk management system is designed to identify the risks it faces and has measures in place to keep those risks to an acceptable minimum. The existence of risk presents both threats and opportunities to the Company.

Risk owners have been assigned responsibility for the identified risks in the Risk Register. The Company's risk assessment matrix is used as the benchmark in planning and implementing the risk management measures. It takes into consideration the nature, scale and complexity of the business.

The risk management process consists of the following main elements:

a. **Identify**: identify a risk (threats or opportunities) and document the risks captured by the risk register owner.

b. **Assess:** the primary goal is to document the net effect of all identified threats and opportunities, by assessing:

    - Likelihood of threats and opportunities (risks);
    - Impact of each risk;
    - Proximity of threats; and
    - Prioritization based on scales.

c. **Plan:** preparation of management responses to mitigate threats and maximize opportunities.

d. **Implement:** risk responses are actioned.

e. **Monitor and Review:** monitor and review the performance of the risk management system and changes to business initiatives.

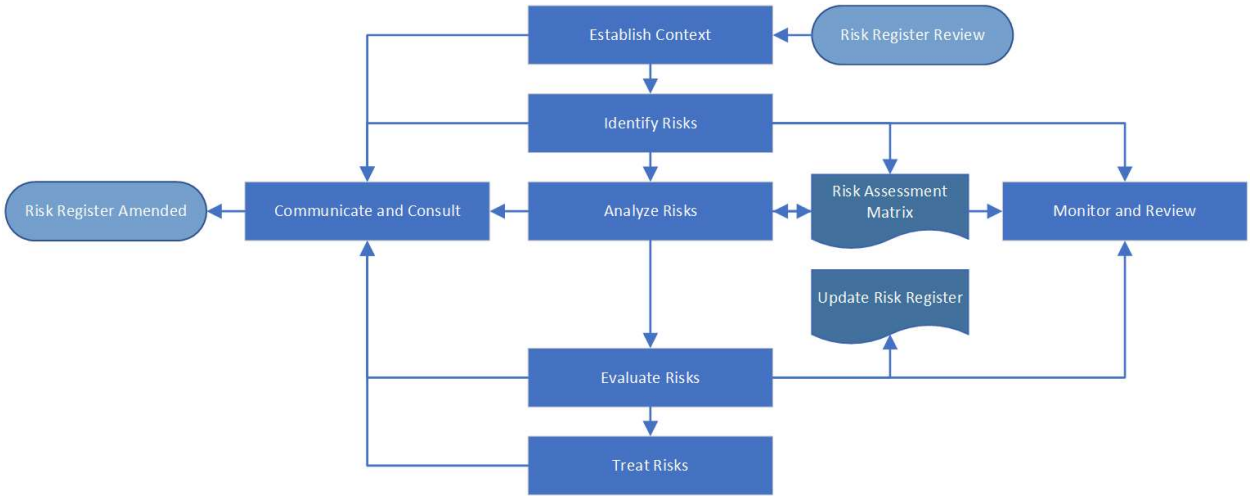
f. **Communicate:** provide regular reports to management team / Audit and Risk Committee at agreed times.

Risks are effectively managed by the Company through the effective implementation of various controls, which include:

- Board approved risk management framework;
- Documented policies and procedures;
- Maintenance of registers;
- Implementation of risk-based systems and processes;
- Ongoing monitoring of regulatory obligations;
- Checklists to guide activities and project plans to record actions; and
- Internal and external reporting.

2. Requirements

a. Overview



b. Risk Management Process

The risk management system is dynamic and is designed to adapt to the Company's developments and any changes in the risk profile over time. Compliance measures are used as a tool to address identified risks.

The risk management system is based on a structured and systemic process which takes into account the Company's internal and external risks.

The main elements of the risk management process are as follows:

- **Communicate and consult** – communicate and consult with internal and external stakeholders as appropriate at each stage of the risk management process and concerning the process as a whole.

- **Establish the context** – establish the external, internal and risk management context in which the rest of the process will take place – the criteria against which risk will be evaluated should be established and the structure of the analysis defined.

- **Identify risks** – identify where, when, why and how events could prevent, degrade, delay or enhance the achievement of the Company's objectives.

- **Record risks** – document the risks that have been identified in the risk register.

- **Analyze risks** – identify and evaluate existing controls. Determine consequences and likelihood and hence the level of risk by analyzing the range of potential consequences and how these could occur.

- **Evaluate risks** – compare estimated levels of risk against the pre-established criteria and consider the balance between potential benefits and adverse outcomes. This enables decisions to be made about the extent and nature of treatments required and about priorities.

- **Treat risks** – develop and implement specific cost-effective strategies and action plans for increasing potential benefits and reducing potential costs.

- **Monitor and review** – it is necessary to monitor the effectiveness of all steps of the risk management process. This is important for continuous improvement. Risks and effectiveness of treatment measures need to be monitored so that changing circumstances do not alter priorities.

The Company's risks may come from any internal or external event which, if it occurs, may affect the ability to efficiently and effectively operate in the financial services industry:

- **Internal risks** – those risks that specifically relate to the Company's business itself and as such as generally within its control. They include risks such as employee related risks, strategic risks, and financial risks.
- **External risks** – those risks that are outside the control of the Company. They include risks such as market conditions and legislative change.

Risks are effectively managed by the Company through the effective implementation of various controls, which include:

- Board approved risk management framework;
- Maintenance of risk register; and
- Regular review of risks and controls, particularly as the business changes.

Risk management can be applied at many levels in an organization. It can be applied at a strategic level and operational level. It may be applied to specific projects, to assist with specific decisions or to manage specific recognized risk areas.

c. Risk Management Methodology

The methodology adopted by the Company for managing and treating its risks can be defined as follows:

1. Document a risk management framework (i.e. the context)

2. Identify the general activities involved in running the business (i.e. risk categories)

3. Identify the risks involved in undertaking the specific business activity by asking the questions:

    a. What could happen?
    b. How and why could it happen?

4. Rate the likelihood of the business activity not being properly performed. Likelihood is assessed to the assumption that there are no existing risk management and compliance processes in place. It is assessed as either **Almost Certain, Likely, Possible, Unlikely** and **Rare**.

5. Rate the consequence of not properly performing the business activity - damage can be quantified in terms of financial loss to investors and/or the Company itself. It is assessed as **Catastrophic, Major, Severe, Serious** and **Minor**.

6. Assign the inherent risk rating based on a combination of the risk rating. Low and Moderate risks may be considered acceptable and therefore minimal further work on these risks may be required. The rating may be assessed as **Critical, High, Significant, Moderate** and **Low**.

7. Decide whether a control (e.g. policy, procedure, checklist, reporting mechanism or account reconciliation) is necessary given the level of risk, based on likelihood and consequences and if so, identify control.

8. Assess whether the existing controls are adequate and allocate the responsibility of monitoring the control to treat the risk. This will integrate risk management and compliance to daily activities and facilitate appropriate control of operational risk.

9. Raise awareness about managing risks across the organization through communicating the policy and responsibilities.

10. Routinely monitor and review ongoing risks so can risk can be effectively managed.

The Risk Assessment Matrix and Risk Register format are shown in Appendix A.

d. Risk Assessment

The Company Assessment Panel will meet regularly to review and evaluate content and currency of the Company examinations. Where appropriate, they will implement requisite changes and submit their findings to the CEO and as warranted.

The CEO will oversee and regularly evaluate all aspects of business activity to ensure operations are carried out responsibly, openly, independently and objectively and that all applicant companies and individuals as well as those with previous certification is treated alike. This will guarantee that Company certification maintains its high standards and integrity.

Quarterly, the CEO will meet with the assessment team, under the direction of the CEO. At this meeting, they will complete a Quarterly Risk Assessment.

Annually, the CEO will meet with the assessment team, under the direction of the CEO. At this meeting, they will complete an Annual Risk Assessment.

Quarterly Risk Assessment Task Checklist	Responsible Role

e. Assess the operational visibility of Cloud Operations and the Security Incident Response Team. In addition to assessing risks in business operations the Assessment Panel must: **i.** Determine whether the Cloud Operations Manager has provided: • Weekly/Monthly Security Testing Reports for the past 3 months • Provided all Change Requests for the past 3 months **f.** Determine whether the Program Manager has provided: • Incident Response Log for the past 3 months • Monthly POA&M for the past 3 months.	• Assessment Panel • Cloud Operations Manager • Program Manager
g. Assess the effectiveness of controls in Cloud Operations and Security Incident Response: **i.** Assess the effectiveness of controls in Cloud Operations and risks including but not limited to: • High Impacts Vulnerabilities have not been remediated within 30 days after identification in reports. • Moderate Impact Vulnerabilities have not been remediated within 90 days after identification in reports • Low Impact Vulnerabilities have not been remediated within 180 days after identification in reports • Multiple recurrences of vulnerabilities • Insufficient Notice of Planned Change • Late or delayed Notification for Emergency Change Requests • Undocumented/Unreported Changes	• Assessment Panel

• Degradation of the Change Management and Change Control Processes **h.** Assess the effectiveness of controls in Security Incident Response and risks including but not limited to: • Late Incident Notification • Any incident with recurring type and/or cause • Incident Frequency • Timely and Ongoing Notification of Attacks	
i. The Assessment Panel must update the Risk Register in Accordance with the Risk Assessment Methodology defined in Section 2c. **j.** The Assessment Panel must document any deficiency identified based on the risk criteria defined in Task 1 and 2.	• Assessment Panel
k. The CEO must formally review the Quarterly Assessment Report and Risk Register to ensure it has been completed in accordance with the Risk Assessment Methodology defined in Section 2c. **l.** The CEO will escalate any deficiency identified by the Assessment Panel in Task 3 to the CEO and the Audit and Risk Committee within 3 Business Days of initial identification. **m.** The CEO will distribute the Quarterly Risk Assessment Report and Risk Register to the CEO and the Audit and Risk Committee within 10 Business Days of the Assessment Panel's Quarterly Meeting.	• CEO

Annual Risk Assessment Task Checklist	Responsible Role
n. The Assessment Panel will complete preparation tasks for the Annual Risk Assessment. This includes: ▪ Identify the Purpose of the Annual Risk Assessment ▪ Identify the Scope of the Annual Risk Assessment ▪ Identify organizational applicability ▪ Time frame supported ▪ Architectural/Technology Considerations ▪ Identify the specific assumptions and constraints under which the risk assessment is conducted ▪ Identify the Information Sources ▪ Source of Descriptive information ▪ Source of Threat information ▪ Source of Vulnerability information ▪ Source of Impact Information ▪ Identify the risk model and analytic approach to be used in the risk assessment.	• Assessment Panel
o. Conduct the Risk Assessment: ▪ Identify Threat Sources including but not limited to: ▪ Previous risk or threat assessments ▪ Open source or classified threat reports ▪ Threat information related to organizational governance ▪ Threat information related to core mission/business functions ▪ Threat information related to management/operational policies ▪ Threat information related to procedures ▪ Threat Information related to facilities ▪ Threat Information related to external mission/business relationships	• Assessment Panel

▪ Threat information related to mission/business processes ▪ Threat information related to common infrastructure ▪ Threat information related to support services ▪ Threat information related to common controls ▪ Threat information related to external dependencies ▪ Threat information related to information systems ▪ Threat information related to information technologies ▪ Threat information related to information system components ▪ Threat information related to applications ▪ Threat information related to environment of operation ▪ Threat information related to adversarial threats ▪ Threat information related to non-adversarial threat sources ▪ Threat information related to accidents ▪ Threat information related to structural threats ▪ Threat information related to environmental threats **p.** Identify Threat Events including but not limited to the following categories: ▪ Threat Events identified by Threat Sources ▪ Threat Events identified in previous risk assessments ▪ Incident Reports/Incident Logs ▪ Reconnaissance and information gathering ▪ Crafting or creating attack tools ▪ Delivering, inserting, installing malicious capabilities ▪ Exploitation and Compromise	

▪ Conducting direct or coordinated attacks ▪ Successful attacks causing adverse impacts or obtaining information ▪ Maintaining presence or set of capabilities ▪ Coordination of a campaign ▪ Spill of sensitive information ▪ Mishandling of critical and/or sensitive information by authorized users ▪ Incorrect privilege settings ▪ Communications contention ▪ Unreadable display ▪ Earthquake at primary facility ▪ Fire at primary facility ▪ Fire at backup facility ▪ Hurricane at primary facility ▪ Hurricane at backup facility ▪ Resource depletion ▪ Introduction of vulnerabilities into software products ▪ Disk Error ▪ Pervasive disk error ▪ Windstorm/tornado at primary facility ▪ Windstorm/tornado at backup facility **q.** Identify vulnerabilities including but not limited to the following categories: ▪ Organizational Level ▪ Mission/Business Process level ▪ Information System Level **r.** Identify predisposing conditions including but not limited to the following categories: ▪ Information Related ▪ Technical ▪ Operational/Environmental **s.** Determine the likelihood that threat events of concern result in adverse impacts including but	

not limited to the following considerations: ▪ The characteristics of the threat sources could initiate the events ▪ The vulnerabilities/predisposing conditions identified ▪ The organizational susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events **t.** Determine the adverse impacts from threat events of concern, considering: ▪ The characteristics of the threat sources could initiate the events ▪ The vulnerabilities/predisposing conditions identified ▪ The organizational susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events **u.** Determine the risk to the organization from threat events of concern considering the impact that would result from the events and the likelihood of the events occurring. Determination of risk will be conducted in accordance with the Risk Management Methodology defined in the Risk Management Policy and Procedure.	
v. The Assessment Panel must update the Risk Register in Accordance and distribute the Annual Risk Assessment Report. **w.** The CEO must formally review the Annual Risk Assessment Report and Risk Register to ensure it has been completed in accordance with the Risk Assessment Methodology defined in Section 2c. **x.** The CEO will distribute the Annual Risk Assessment Report to the CEO, Audit and Risk Committee and Board of Directors for final review.	• Assessment Panel • CEO • CEO • Board of Directors • Audit and Risk Committee

y. The CEO will distribute the approved Annual Risk Assessment Report to any external authorized officials.	
z. The Board of Directors, Audit and Risk Committee, and CEO will formally review the membership of the Assessment Panel within 30 days of Annual Risk Assessment Report completion. **aa.** The Board of Directors, Audit and Risk Committee, and CEO will determine whether the Annual Risk Assessment Report and Quarterly Risk Assessment Report effectively monitored organizational risk factors. **bb.** The Board of Directors, Audit and Risk Committee, and CEO will add or remove Assessment Panel members to ensure subsequent risk assessments will effectively monitor and report organizational risk factors.	• Board of Directors • Audit and Risk Committee • CEO
cc. The Board of Directors, Audit and Risk Committee, and CEO will formally review the Risk Management Policy and Procedure within 30 days of Annual Risk Assessment Report completion. **dd.** The CEO will update the Risk Management Policy and Procedure based on recommendations of the Board of Directors and Audit and Risk Committee. **ee.** The CEO will approve the Risk Management Policy and Procedure.	• Board of Directors • Audit and Risk Committee • CEO • CEO

3. Responsibilities

The Program Manager approves the Risk Management Policy and Procedure. The Program Manager also is responsible for ensuring the development, implementation, and maintenance of the Risk Management Policy and Procedure.

Company management, including senior management and department managers, is accountable for ensuring that the Risk Management Policy and Procedure is properly communicated and understood within their respective organizational units. Company management also is responsible for defining, approving and implementing procedures in its organizational units and ensuring their consistency with the Risk Management Policy and Procedure.

Asset Owners (Owners) are the managers of organizational units that have primary responsibility for information assets associated with their functional authority. When Owners are not clearly implied by organizational design, the CEO will make the designation. The Owner is responsible for defining processes and procedures that are consistent with the Risk Management Policy and Procedure; defining the access control requirements for information assets associated with their functional authority; processing requests associated with Company-approved access request procedure; determining the level of access and authorizing access based on Company-approved criteria; ensuring the revocation of access for those who no longer have a business need to access information assets; and ensuring the access controls and privileges are reviewed at least annually.

Asset Custodians (Custodians) are the managers, administrators and those designated by the Owner to manage process or store information assets. Custodians are responsible for providing a secure processing environment that protects the confidentiality, integrity, and availability of information; administering access to information assets as authorized by the Owner; and implementing procedural safeguards and cost-effective controls that are consistent with the Risk Management Policy and Procedure.

Users are the individuals, groups, or organizations authorized by the Owner to access to information assets. Users are responsible for familiarizing and complying with the Risk Management Policy and Procedure and associated guidelines; following Company-approved processes and procedures to request and obtain access to information assets; ensuring authorization credential such as password and tokens are not written down or stored in a place where unauthorized persons might discover them; reporting immediately to the **Information Security Helpline at 703-879-7996** when authorization credentials

have been or may have been compromised; and maintaining the confidentiality, integrity and availability of information accessed consistent with the Owner's approved safeguards while under the User's control.

4. Enforcement and Exception Handling

Failure to comply with the Risk Management Policy and Procedure and associated guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the Risk Management Policy and Procedure should be submitted to the Company Program Manager. Exceptions shall be permitted only on receipt of written approval from the Program Manager. The Program Manager will periodically report current status to the Company CEO or its designee.

5. Review and Revision

The Risk Management Policy and Procedure will be reviewed and revised in accordance with the **Information Security Program Charter**.

Recommended: _____

Signature

Pakkirisankar Jagannath

Program Manager

Approved: _____

Signature

Anil Sharma

CEO

Appendix A – Risk Assessment Matrix and Risk Register

Risk Consequence Severity

Consequence Type	Minor	Serious	Severe	Major	Catastrophic
Financial Loss	< 1m	1m-5m	5m-10m	>10m	Threatens viability of Company
Reputation Loss					

Likelihood Probability & Frequency

Likelihood Rating	Description	Probability
Almost Certain	Known to happen often	> 95%
Likely	Could easily happen	50% - 95%
Possible	Could happen & has occurred before	15% - 50%
Unlikely	Hasn't happened yet but could	5% - 15%
Rare	Conceivable, but only in extreme circumstances	> 5%

Control Effectiveness

Control Effectiveness	Description
Effective	The control design meets the control objective and the control is operating the majority of the time
Partially Effective	The control design mostly meets the control objective, and/or the control is normally operational but occasionally is not applied when it should be, or not as intended
Ineffective	The control design does not meet the control objective, and/or the control is not applied or is applied

Risk Assessment Matrix

Likelihood	Likelihood Rating	Minor	Serious	Severe	Major	Catastrophic
	Almost Certain	Moderate	High	Critical	Critical	Critical
	Likely	Moderate	Significant	High	Critical	Critical
	Possible	Moderate	Moderate	Significant	High	Critical
	Unlikely	Low	Low	Moderate	Significant	Critical
	Rare	Low	Low	Moderate	Moderate	High

Critical	Extreme risk - detailed research and management planning required at senior levels
High	High risk- immediate senior management attention needed

Significant	Significant risk - Senior management attention needed
Moderate	Moderate risk - Management responsibility must be specified
Low	Low risk - Manage by routine procedures

Risk Register

ID	Risk	Owner	Consequences	Likelihood	Inherent Risk Level	Controls	Control Effectiveness
	Risk Area						
1	Risk name and description.						
2							
3							
4							
5							