Risk Management Policy

1. DOCUMENT OWNERSHIP AND APPROVAL

The GRC Team:

- Leads the development of the policy.
- Ensures that the policy aligns with industry standards and best practices.
- Coordinates with other departments to identify risks and necessary controls.

Chief Information Officer (CIO) :

- Provides final technical approval and ensures alignment with the organization's IT strategy.

2 SCOPE AND CONTEXT

This policy applies to all employees, contractors, and third-party service providers who have access to the organization's information systems, networks, and data.

3. Roles and Responsibilities

- **Senior Management**: Provide oversight and ensure the allocation of resources for effective risk management.
- **IT Security Team**: Lead the risk management process, conduct risk assessments, and implement security controls.
- **Risk Management Committee**: Review risk assessments, approve risk treatment plans, and monitor risk management activities.
- **Employees and Contractors**: Adhere to the risk management policy, report potential risks, and participate in training and awareness programs.

4. RISK MANAGEMENT REQUIREMENTS

a. Risk management will be incorporated into the strategic and operational planning processes of the company;
b. Risk and the management of risk will be identified and monitored according to the company's risk management policy;
c. Risk assessments will be conducted on all new ventures and projects prior to commencement to ensure alignment with the company's risk appetite and organisational objectives;
d. Risks will be identified, reviewed and monitored on an ongoing basis as outlined in Sections 10 to 15 of this policy;
e. Relevant risks that are identified will be recorded within company's risk management register;

5. Components of Risk Criteria

1. **Likelihood**: The probability that a risk event will occur.

2. **Impact**: The potential consequences or severity of a risk event if it occurs.
3. **Risk Levels**: The combination of likelihood and impact to determine the overall risk level.

4. **Risk Appetite**: The amount and type of risk that the organization is willing to accept in pursuit of its objectives.

Risk Level	Description	Action Required
Low	Acceptable risk, no action needed	Accept and monitor
Medium	Acceptable risk, but requires monitoring and periodic review	Implement routine controls and monitoring
High	Risk is significant, requires mitigation	Develop and implement mitigation plans
Critical	Unacceptable risk, requires immediate action	Immediate action to mitigate or avoid the risk

5. Event Identification

Event identification is a critical component of risk management, where potential events that could impact the organization are recognized and documented. These events can be internal or external and may positively or negatively affect the achievement of organizational objectives.

Steps for Event Identification

a. **Understand the Organization's Context**
   - **Internal Context**: Consider the organization's internal environment, including its mission, objectives, structure, processes, and culture.
   - **External Context**: Assess external factors such as industry trends, regulatory environment, technological changes, and socio-political factors.

b. **Identify Information Assets**
   - Catalog all information assets, including hardware, software, data, networks, and intellectual property.
   - Classify these assets based on their criticality to the organization's operations and objectives.

c. **Identify Potential Threats**

- **Cyber Threats**: Malware, ransomware, phishing, zero-day exploits, denial-of-service attacks, insider threats.
- **Physical Threats**: Natural disasters (floods, earthquakes), theft, vandalism, and physical intrusion.
- **Operational Threats**: Human error, system failures, supply chain disruptions.

d. Identify Vulnerabilities

- Conduct vulnerability assessments and penetration testing to identify weaknesses in systems, applications, and networks.
- Review past incidents and audit reports to identify recurring vulnerabilities.

e. Analyze Historical Data

- Examine historical data on past incidents and security breaches to identify patterns and common threats.
- Use industry reports and threat intelligence feeds to stay informed about emerging threats.

f. Engage Stakeholders

- Conduct workshops and brainstorming sessions with stakeholders, including IT, security teams, management, and end-users, to gather insights on potential events.
- Use questionnaires and surveys to collect input from a broader audience.

g. Use Structured Techniques

- **Scenario Analysis**: Develop and analyze scenarios that could lead to significant events, considering worst-case and best-case situations.

h. Document Events

- Record identified events in a centralized risk register or database.
- Include detailed descriptions, potential causes, affected assets, and possible consequences.

i. Categorize Events

- Group events into categories such as operational, strategic, financial, compliance, and reputational to better understand their nature and impact.

j. Regular Review and Update

- Continuously monitor the environment for new threats and vulnerabilities.
- Periodically review and update the list of identified events to reflect changes in the organization's context and threat landscape.

7. Key questions that can be used to identify and control risks: What, when, where, why and how risks are likely to occur and who might be involved; What is the source of each risk; What are the consequences of each risk; What controls presently exist to

mitigate each risk; To what extent are controls effective; What alternative, appropriate controls are available; What are the public institution's obligations (external and internal); What is the need for research into specific risks, scope for such research and resources required; What is the reliability of the information; and Is there scope for bench-marking with peer or related public and/or private sector institutions

8. Risk Assessment

1. Identify Assets

- **Inventory Assets**: List all physical and digital assets, including hardware, software, data, network components, and intellectual property.
- **Classify Assets**: Categorize assets based on their criticality and importance to the organization's operations.

2. Identify Threats

- **Internal Threats**: Include threats from within the organization such as employee errors, insider attacks, and system failures.
- **External Threats**: Include threats from outside the organization such as cyberattacks (e.g., phishing, malware, DDoS), natural disasters, and supply chain disruptions.

3. Identify Vulnerabilities

- **Technical Vulnerabilities**: Weaknesses in software, hardware, or network configurations that could be exploited.
- **Operational Vulnerabilities**: Gaps in policies, procedures, and controls.
- **Human Vulnerabilities**: Lack of employee training, awareness, or adherence to security protocols.

4. Determine Likelihood

- Assess the probability of each identified threat exploiting a vulnerability. Use historical data, threat intelligence, and expert judgment to estimate likelihood.
- **Likelihood Scale**:

Table 3.5.3: Likelihood matrix

		Probability of vulnerability being breached				
		Very Low	Low	Medium	High	Very High
Frequency of threat occuring	Very Low	Very Low	Very Low	Low	Low	Medium
	Low	Very Low	Low	Low	Medium	High
	Medium	Low	Low	Medium	High	High
	High	Low	Medium	High	High	Very High
	Very High	Medium	High	High	Very High	Very High

5. Determine Impact

- Assess the potential consequences if a threat exploits a vulnerability. Consider financial, operational, reputational, and legal impacts.
- **Impact Scale**:

EXAMPLE: RISK IMPACT SCORING PARAMETERS:

Rate	*Impact*	*Impact measure*	*Enhanced Rating Scales*
5	Critical (Catastrophic impact)	Negative outcomes or missed opportunities that are of critical importance to the achievement of the objectives.	**Extremely High Significance** Strategic objectives cannot be achieved, resulting in significant financial impact and questions about future viability.
4	Major (Very material impact)	Negative outcomes or missed opportunities that are likely to have a relatively substantial impact on the ability to meet objectives.	**Highly Significant** Difficult to achieve strategic objectives and / or material financial impact.
3	Moderate impact	Negative outcomes or missed opportunities that are likely to have a relatively moderate impact on the ability to meet objectives.	**Moderately Significant** Noticeable challenges to a strategic objectives.
2	Minor impact	Negative outcomes or missed opportunities that are likely to have a relatively low impact on the ability to meet objectives.	**Slightly Significant** Small material impact
1	Insignificant	Negative outcomes or missed opportunities that are likely to have a negligible impact on the ability to meet objectives.	**Not Significant** No discernable impact. Neither a strategic nor financial impact.

6. Evaluate Risk Levels

- **Risk Matrix**: Combine likelihood and impact to determine the overall risk level.

		Impact Level				
		Very Low	**Low**	**Medium**	**High**	**Very High**
Likelihood	Very Low	Very Low	Very Low	Low	Low	Medium
	Low	Very Low	Low	Low	Medium	High
	Medium	Low	Low	Medium	High	High
	High	Low	Medium	High	High	Very High
	Very High	Medium	High	High	Very High	Very High

7. Prioritize Risks

- Prioritize risks based on their overall risk level. Focus on addressing high and critical risks first.

8. Develop Risk Mitigation Strategies

- **Avoidance**: Eliminate the risk by removing the cause.
- **Mitigation**: Reduce the likelihood or impact of the risk through controls and safeguards.
- **Transfer**: Shift the risk to a third party (e.g., insurance).
- **Acceptance**: Acknowledge the risk and decide to accept it without additional action.

9. Implement Controls

- Implement technical, administrative, and physical controls to mitigate identified risks.
- Ensure that controls are documented, communicated, and enforced.

10. Monitor and Review

- Continuously monitor the risk environment and the effectiveness of controls.
- Regularly review and update the risk assessment to adapt to new threats and vulnerabilities.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.
Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

	Treat	Vulnerability	Likelihood	Impact	Initicial Risk	Controls	Residual Risk
Phishing Attack	Medium	High	High	High	High	Employee training programs, email filtering	Medium
Ransomware Attack	Low	High	Medium	High	High	Regular updates and patch management, backups	Low
Data Breach	Medium	High	High	High	High	Strong access controls, data encryption	Medium
Insider Data Theft	Very Low	Medium	Low	High	Medium	Strict access controls, user activity monitoring	Low