TECH THAT MATTERS

Elevaite365

Risk Management Procedure

Version 1.0

PURPOSE

This Risk Management Procedure Policy defines the actions required to address the Elevaite365 (herein referred to as “the organization”), information security risks, and opportunities. It establishes a structured approach to identifying, analyzing, controlling, and monitoring information security risks to achieve the Organization’s information security and privacy objectives. By implementing this policy, the Organization aims to protect its assets, ensure compliance with regulatory requirements, and support its strategic and operational goals.

SCOPE

This policy applies to all organization IT systems that process, store, or transmit confidential, private, or business-critical data. It encompasses:

1. All IT Systems: Systems that handle confidential, private, or business-critical data.
2. Risk Considerations: Risks impacting medium-to-long-term goals and those encountered in day-to-day service delivery.
3. Risk Management Systems: Processes designed to achieve maximum benefit without increasing bureaucratic burdens or affecting core service delivery.
4. Materiality of Risk: Focus on material risks in developing risk management systems and processes.
5. Applicable Individuals and Entities: All employees of the Organization and external parties, including consultants, contractors, business partners, vendors, suppliers, outsourced service providers, and other third-party entities with access to the Organization’s networks and system resources.

DEFINITIONS

- CISO: Chief Information Security Officer – The executive overseeing the Organization’s information and data security strategies and implementations.
- CTO: Chief Technology Officer – The executive responsible for the technological direction of the Organization, including the development and implementation of technology strategies.
- PII: Personally Identifiable Information – Information that can be used to identify an individual on its own or when combined with other information.
- Likelihood: The probability that a given event will occur.
- Impact: The extent to which a risk event might affect the Organization.
- Acceptance Criteria: The limits above which the Organization will not tolerate risk.
- Risk Register: A tool used to document identified risks, their assessment, and their actions to manage them.
- Risk Treatment PI: A plan outlining the actions to mitigate, transfer, accept, or avoid identified risks.
- Risk Assessment: Identifying, analyzing, and evaluating risks to determine their potential impact on the Organization.
- Risk Appetite: The amount and type of risk the Organization is willing to pursue or retain.
- Risk Tolerance: The acceptable variation around objectives that the Organization is willing to allow

RESPONSIBILITIES

Chief Information Security Officer (CISO)

- Risk Acceptance: Ultimately responsible for accepting and/or treating any risks to the Organization.
- Approval Authority: Can approve the avoidance, remediation, transference, or acceptance of any risk cited in the Risk Register.
- Strategic Oversight: Ensures alignment of risk management with the Organization’s strategic objectives.

Chief Technology Officer (CTO)

- Risk Identification: Identifies and develops treatment plans for all information security-related risks.
- Risk Treatment Plans: Oversees the creation and implementation of risk treatment plans.
- Communication: Communicates risks to top management and ensures risk treatments are adopted by executive direction.

Information Security Group (ISG)

- Policy Implementation: Develops and enforces the Risk Management Procedure Policy in collaboration with relevant departments.
- Monitoring and Compliance: Ensures adherence to the policy through regular audits and inspections.
- Training and Awareness: Conducts training sessions to educate employees and contractors about best practices for risk management.

- Incident Response Coordination: Coordinates responses to identified risks and security incidents.

IT and DevOps Teams

- Risk Identification: Assist in identifying and assessing information security risks.
- Implementation: Implement risk treatment plans as directed by the CTO and CISO.
- Monitoring: Continuously monitor IT systems for emerging risks and vulnerabilities.

POLICY

Organizations have developed processes to identify risks that may restrict achieving their strategic and operational objectives. The Organization ensures that it has the means to identify, analyze, control, and monitor strategic and operational risks using this risk management policy based on best practices. The risk management policy and procedure are reviewed regularly, and internal audit functions are responsible for ensuring:

- The risk management policy is applied to all applicable areas of the Organization.
- The risk management policy and its operational application are regularly reviewed.
- Non-compliance is reported to appropriate company officers and authorities.

RISK CATEGORIES

The organization will consider and assess risks across the organization. The following risk categories should be evaluated:

- Reputational: Risks that could damage the Organization's reputation.
- Contractual: Risks arising from contractual obligations and agreements.
- Regulatory/Compliance: Risks related to non-compliance with laws, regulations, and standards.
- Economic/Financial: Risks that could impact the Organization's financial stability.
- Fraud: Risks of fraudulent activities within or against the Organization.
- Privacy: Risks concerning the protection of personal and sensitive information.
- Impact on People: Risks that could affect employees, customers, or other stakeholders.
- Use of Cloud Services: Risks associated with utilizing cloud-based services and infrastructure.
- Operational Capacity: Risks that could hinder the Organization's ability to deliver services effectively.

Each risk will be assessed for its likelihood and impact. Both impact and probability are evaluated on a scale of 1-5. The effect can range from 1 ("Very low impact") to 5 ("Very high impact"), and likelihood can range from 1 ("Very unlikely") to 5 ("Very likely").

RISK CRITERIA

The criteria for determining risk are based on an event's combined likelihood and impact adversely affecting the confidentiality, availability, integrity, or privacy of organizational and customer information, personally identifiable information (PII), or business information systems. For all risk inputs, such as risk assessments, vulnerability scans, penetration tests, bug bounty programs, etc., Organization management reserves the right to modify risk rankings based on the evaluation of the nature and criticality of the system processing and the nature, criticality, and exploitability (or other relevant factors and considerations) of the identified vulnerability.

RISK RESPONSE, TREATMENT, AND TRACKING

Risks will be prioritized and maintained in a Risk Register, where they will be mapped using the approach contained in this policy. The following responses to risk should be employed:

1. **Remediate**: Take actions or employ strategies to reduce the risk.
2. **Accept**: Decide to accept and monitor the risk at present. This may be necessary for some risks arising from external events.
3. **Transfer**: Pass the risk on to another party, such as through contractual terms or insurance.
4. **Avoid**: Cease the activity or change it in such a way as to eliminate the risk.

Where an organization chooses a risk response other than "Accept" or "Avoid," a Risk Treatment Plan shall be developed.

RISK MANAGEMENT PROCEDURE

The procedure for managing risk will meet the following criteria:

1. Risk Register and Treatment Plan:
    - Maintain a Risk Register and Treatment Plan to document and manage identified risks.
2. Risk Ranking:
    - Risks are ranked by Likelihood and Impact as Critical, High, Medium, and Low.
3. Overall Risk Determination:
    - Overall risk is determined through a combination of likelihood and impact.
4. Prioritized Risk Response:
    - Respond to risks in a prioritized fashion. Remediation priorities will consider risk likelihood and impact, cost, work effort, and resource availability. Multiple remediations may be undertaken simultaneously.
5. Regular Reporting:
    - Regular reports will be made to the organization's senior leadership to ensure risks are being mitigated appropriately and in alignment with business priorities and objectives.

APPENDIX A

RISK ASSESSMENT PROCESS

The following is a high-level overview of the process used by Organizations to assess and manage information security-related risks.

The risk assessment process is comprised of the following steps:

1. Prepare for the assessment
2. Conduct the assessment
3. Communicate the assessment
4. Maintain the assessment

Step 1: Prepare for the Assessment

In this step, the objective is to establish the context for the risk assessment. This can be accomplished by performing the following

1. Identify the purpose of the assessment
    - Determine the information the assessment intends to produce and the decisions the assessment intends to support.
2. Identify the scope of the assessment.
    - Determine the applicable organizational function or process, the associated time frame, and any applicable architectural or technological considerations.
3. Identify any assumptions or constraints associated with the assessment
    - Determine assumptions in key areas relevant to the risk assessment, including
        a. Organizational priorities
        b. Business objectives
        c. Resource availability
        d. Skills and expertise of the risk assessment team
4. Identify sources of information.
    - Architectural/technological diagrams and system configurations
    - Legal and regulatory requirements
    - Threat Sources

- Threat Events
- Vulnerabilities and influencing conditions
- Potential Impacts
- Existing Controls

Step 2: Conduct the Assessment

This step aims to produce a list of information security-related risks that can be prioritized by risk level and used to inform risk response decisions. This can be accomplished by performing the following:

1. Identify Threat Sources
    - Determine and characterize threat sources relevant to and of concern to Othe organization, including but not limited to:
        a. Human (Intentional or Unintentional / Internal or External)
        b. Environmental
        c. Natural
        d. System or Equipment
2. Consider the following when identifying threat sources:
    - Capability
    - Motive / Intent
    - Intentionally targeted people, processes, and/or technologies.
    - Unintentionally targeted people, processes, and/or technologies.
3. Identify Threat Events
    - Determine what threat events could be produced by the identified threat sources that could potentially impact the Organization.
4. Consider the relevance of the events and the sources that could initiate the events.
5. Identify Vulnerabilities
    - Determine the vulnerabilities associated with people, processes, and technologies that the identified threat sources and events could exploit.
6. Consider any influencing conditions that could affect and aid in successful exploitation.
7. Determine Likelihood
    - Determine the likelihood that the identified threat sources would initiate the identified threat events and could successfully exploit any identified vulnerabilities.
8. The vulnerabilities and/or influencing conditions identified
9. Organization exposure is based on any safeguards/countermeasures planned or implemented to prevent or mitigate such events.
10. Determine Impact
    - Determine the impact on Required Company Name’s business objectives, operations, assets, individuals, customers, and/or other organizations by considering the following:
        a. Business / Operational Impacts
        b. Financial Damage
        c. Reputation Damage
        d. Legal or Regulatory Issues
11. When determining impact, consider any safeguards/countermeasures planned or implemented by the Organization that would mitigate or lessen the impact.
12. Determine Risk
13. Determine the overall information security-related risks to the Organization by combining the following:
    - The likelihood of the event occurring. (L)
    - The impact that would result from the event. (I)

Risk Score = Likelihood x Impact

14. The risk to the Organization is proportional to the likelihood and impact of an event.
    - Higher Risk Event: This is more likely to occur, resulting in a more significant impact.
    - Lower Risk Event: This is less likely to occur, and the resulting impact will be minimal, if any.

Step 3: Communicate and Share the Risk Assessment Results

This step ensures that decision-makers across the Organization and executive leadership have the appropriate risk-related information needed to inform and guide risk decisions.

1. Communicate the Results
    - Communicate the risk assessment results to the organization's decision-maker and executive leadership to help drive risk-based decisions and obtain the necessary support for the risk response.
2. Share the risk assessment and risk-related information with the appropriate personnel at the Organization to help support the risk response efforts.

Step 4: Maintain the Assessment

In this step, the objective is to keep current with the specific knowledge related to the risks that the Organization incurs. The results of the assessments inform and drive risk-based decisions and guide ongoing risk response efforts.

1. Monitor Risk Factors
    - Conduct ongoing monitoring of the risk factors contributing to changes in risk to the Organization's business objectives, operations, assets, individuals, customers, and/or other organizations.
2. Maintain and Update the Assessment
    - Update existing risk assessments using the results from ongoing monitoring of risk factors and by conducting additional assessments, at minimum annually.

APPENDIX B

Risk Assessment Matrix and Description Key

RISK= LIKELIHOOD * IMPACT	**LIKELIHOOD**				
IMPACT	**Very unlikely: 1**	**Unlikely : 2**	**Somewhat likely: 3**	**Likely: 4**	**Very likely: 5**
Very high impact: 5	**5**	**10**	**15**	**20**	**25**
High impact: 4	**4**	**8**	**12**	**16**	**20**
Medium impact: 3	**3**	**6**	**9**	**12**	**15**
Low impact: 2	**2**	**4**	**6**	**8**	**10**
Very low impact: 1	**1**	**2**	**3**	**4**	**5**

RISK LEVEL	RISK DESCRIPTION

Low (1-7)	A threat event could be expected to have a limited adverse effect on organizational operations, mission capabilities, assets, individuals, customers, or other organizations.
Medium (7-14)	A threat event could be expected to have a profound adverse effect on organizational operations, mission capabilities, assets, individuals, customers, or other organizations
High (15-25)	A threat event could be expected to severely affect organizational operations, mission capabilities, assets, individuals, customers, or other organizations.

LIKELIHOOD OD	LIKELIHOOD DESCRIPTION	RATING (NUMERICAL)
LEVEL		
Very unlikely (1)	A threat event is so unlikely that it can be assumed that its occurrence may not be experienced. A threat source is not motivated or has no capability or controls to prevent or significantly impede the vulnerability from being exploited.	1
Unlikely (2)	A threat event is unlikely, but there is a slight possibility that its occurrence may be experienced. A threat source lacks sufficient motivation or capability, or controls are in place to prevent or impede the vulnerability from being exploited.	2
Somewhat t likely (3)	A threat event is likely, and it can be assumed that its occurrence may be experienced.	3

	A threat source is motivated or poses the capability, but controls are in place that may significantly reduce or impede the successful exploitation of the vulnerability.	
Likely (4)	A threat event is likely, and it can be assumed that its	4

	occurrence will be experienced. A threat source is highly motivated or poses sufficient capability and resources, but some controls are in place that may reduce or impede the successful exploitation of the vulnerability.	
Very likely (5)	A threat event is highly likely, and it can be assumed that its occurrence will be experienced. A threat source is highly motivated or poses sufficient capability or resources. Still, no controls are in place, or controls that are in place are ineffective and do not prevent or impede the successful exploitation of the vulnerability.	5

IMPACT LEVEL	IMPACT DESCRIPTION	RATING (NUMERICAL)
Very low impact (1)	A threat event could be expected to have almost no adverse effect on organizational operations, mission capabilities, assets, individuals, customers, or degradation of mission capability, yet primary functions can still be performed, minor damage, minor financial loss, or a range of effects significant degradation of	1
	mission capability, yet primary functions can still be performed at a reduced capacity; minor damage; minor financial loss; or a range of effects, and impede-severely affect or organizations	
Low impact (2)	A threat event could be expected to have a limited adverse effect, meaning degradation of mission capability, yet primary functions can still be performed; minor damage, financial loss, or range of effects is limited to some cyber resources but no critical resources.	2
Medium impact (3)	A threat event could be expected to have a profound adverse effect, meaning significant degradation of mission capability, yet primary functions can still be performed at a reduced capacity. Minor damage, financial loss, or a range of effects are significant to some cyber and critical resources.	3
High impact (4)	A threat event could be expected to have a severe or catastrophic adverse effect, meaning severe degradation or loss of mission capability and one or more primary functions cannot be performed; major damage; major financial loss; or a range of effects is extensive to most cyber resources and most critical resources.	4

Very high impact (5)	A threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, assets, individuals, other organizations, or the Nation. The impact is sweeping, involving almost all cyber resources.	5

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	-	Initial Release	Borhan	-	-