Cybersecurity & Infrastructure Security Agency

Risk Management Policy

Effective Date: January 1, 2025
Review Date: September 26, 2024
Approved by: Elliot Mason | Chief Risk Officer

1. Purpose

The purpose of this Risk Management Policy is to establish a systematic approach to identifying, assessing, and managing risks that may impact the CISA's objectives and operations.

2. Scope

This policy applies to all employees, departments, and activities within CISA. It covers all types of risks, including operational, financial, strategic, compliance, and reputational risks.

3. Definitions

- **Risk:** The effect of uncertainty on objectives, which can be positive (opportunities) or negative (threats).
- **Risk Management:** The process of identifying, assessing, and controlling risks to minimize their impact.

4. Objectives

- To create a risk-aware culture throughout the organization.
- To protect the organization's assets and reputation.
- To ensure compliance with relevant laws and regulations.
- To enhance decision-making by providing a clear understanding of risks.

5. Risk Management Framework

- **Identification:** Regularly identify potential risks through various methods, including brainstorming sessions, surveys, and industry analysis.
- **Assessment:** Evaluate identified risks based on their likelihood and potential impact, using a standardized risk matrix.
- **Response:** Develop and implement strategies to mitigate identified risks, including avoidance, reduction, sharing, or acceptance.
- **Monitoring:** Continuously monitor risks and the effectiveness of risk management strategies. Review and update risk assessments periodically.

- **Reporting:** Establish a reporting mechanism for risk management activities to keep stakeholders informed.

6. Roles and Responsibilities

- **Board of Directors:** Provide oversight and approve the risk management policy.
- **Risk Management Committee:** Oversee risk management activities, review risk assessments, and recommend policies to the Board.
- **Department Heads:** Ensure that risk management practices are implemented within their areas and report on risks.
- **Employees:** Participate in the risk identification and assessment process and follow established risk management procedures.

7. Training and Awareness

Regular training sessions will be conducted to enhance employees' understanding of risk management principles and practices. Training will be mandatory by all employees under all departments of CISA. Mandatory training must be completed within the allotted time given by a department’s Chief Officer.

8. Review and Revision

This policy is to be reviewed by CISA Executive Leadership annually and revised by the Chief Risk Officer biannually to comply with CISA regulations.

9. Compliance

Failure to comply with this policy may result in disciplinary action and can lead to increased organizational risk.

10. Approval

This policy has been approved by CISA Executive Leadership on September 26, 2024.
