Risk Mangement Policy

Diné College Information Technology

Michael Morrow

Revision History

Version Number	Revision Date
1.0	10/2/2024

Table of Contents

1. Purpose

This section outlines the purpose of the Risk Management Policy, which is to ensure that all technology platforms, systems, and data assets are regularly assessed for risks and vulnerabilities. This policy defines the framework for identifying, evaluating, and mitigating risks to protect the confidentiality, integrity, and availability of organizational information and technology resources.

As technology evolves and new capabilities are introduced, threats to the organization's assets grow more complex. To maintain security and operational resilience, departments and system owners must conduct regular risk assessments, while the Information Security Office (ISO) oversees the risk management process across the organization.

2. Scope

This policy applies to all departments, system owners, IT professionals, and third-party partners who are responsible for managing or operating information systems and technology platforms. It covers all data, applications, infrastructure, and technology services across the organization.

The risk management framework applies to systems and data classified as Confidential Data and Protected Data, as well as any other critical technology assets that support business operations. This policy encompasses risk assessments performed for regulatory compliance, industry standards, or internal governance purposes.

3. Roles and responsibilities

The following roles are responsibilities outline the ownership and actions held by stakeholders in the response process.

Chief Information Officer (CIO)

The CIO is responsible for overseeing the entire risk management program, ensuring that risk assessments are conducted regularly and that identified risks are mitigated appropriately. The CIO reviews major risks and mitigation strategies with senior leadership to ensure organizational priorities align with security goals.

Information Security Officer (ISO)

The ISO is authorized to administer the organization's risk management process and is responsible for developing risk management policies and procedures. The ISO provides tools and guidance for departments and system owners to assess risks and works closely with stakeholders to evaluate high-priority risks.

Department Heads and System Owners

Department heads and system owners are accountable for conducting regular risk assessments of the systems, technologies, and data they manage. They must evaluate risks to their platforms using a

comprehensive approach and develop plans to mitigate identified risks. They are also responsible for implementing controls and following up on risk mitigation efforts.

IT Professionals

IT professionals are responsible for providing technical support and expertise during the risk assessment process. They assist system owners in identifying vulnerabilities, implementing security controls, and ensuring that systems are configured according to the organization's risk management guidelines.

4. Risk Assessment Process

This section provides a detailed framework for conducting risk assessments, ensuring a structured approach to identifying, analyzing, and prioritizing risks across the organization's information systems and technology platforms.

The risk assessment process is a critical component of the overall risk management strategy, designed to evaluate potential risks to the confidentiality, integrity, and availability of technology assets. This process ensures that risks are systematically identified, categorized, and prioritized for mitigation.

4.1 Risk Identification

The first step in the risk assessment process involves identifying potential risks to information systems and data. Departments, system owners, and IT professionals are responsible for identifying risks within their areas of responsibility, using the following approaches:

- Asset Inventory: Begin with a comprehensive inventory of all information systems, applications, and data. Identify critical assets, including those that contain Confidential Data (e.g., Personally Identifiable Information (PII), Protected Health Information (PHI), Payment Card Information (PCI)) and Protected Data.
- Threat Analysis: Evaluate potential threats to these assets. This includes internal threats (e.g., insider misuse, system misconfigurations) and external threats (e.g., hacking attempts, malware, phishing attacks). Emerging threats, such as supply chain risks and third-party vulnerabilities, should also be considered.
- Vulnerability Identification: Assess each system for vulnerabilities that may be exploited by identified threats. This could include unpatched software, outdated systems, poor access control measures, or lack of data encryption.

4.2 Risk Analysis

- Once risks have been identified, they must be analyzed to understand their potential impact on the organization's information assets. This analysis involves:

- Likelihood: Determine the probability of each risk materializing. Likelihood may be influenced by factors such as the presence of controls, the complexity of the threat, and the vulnerability's exposure.
- Impact: Assess the potential impact of each risk on the organization. Impact is measured in terms of the damage it could cause, such as data loss, operational disruption, financial loss, or reputational damage. Critical systems that affect business continuity or public trust should be given higher priority.
- Risk Level Calculation: Use a risk matrix or other risk assessment tools to calculate the overall risk level by combining likelihood and impact scores. The risk level can be categorized as Low, Moderate, High, or Critical. For example.

Likelihood	Impact	Risk Level
High	High	Critical
High	Low	Moderate
Low	High	Moderate
Low	Low	Low

This analysis helps in determining which risks need immediate attention and which can be monitored over time.

4.3 Risk Prioritization

After analyzing risks, they must be prioritized based on their risk level. The prioritization process ensures that high-risk vulnerabilities are addressed first, particularly those that could result in significant data breaches or operational downtime.

- High and Critical Risks: These risks must be addressed immediately. A detailed mitigation plan must be developed to reduce the likelihood or impact of these risks, and system owners must ensure that the required controls are implemented without delay.
- Moderate Risks: These risks should be managed with ongoing monitoring and remediation as necessary. Although not urgent, they must be addressed before they can escalate.
- Low Risks: These risks can be accepted with regular monitoring. However, they should not be ignored, as even low risks may compound over time if left unaddressed.

4.4 Risk Mitigation Planning

For each identified risk, a mitigation plan must be created that outlines specific actions to reduce or eliminate the risk. The plan should detail:

- Mitigation Strategies: Determine appropriate security controls to address the risk. These may include technical controls (e.g., firewalls, encryption), administrative controls (e.g., policies, training), and physical controls (e.g., secure facility access).
- Risk Ownership: Assign ownership for the mitigation plan. System owners or department heads are responsible for ensuring that the mitigation strategies are implemented and documented.
- Timelines: Establish clear deadlines for implementing risk mitigation measures, particularly for high and critical risks that require immediate action.
- Residual Risk: After mitigation actions have been taken, there may still be some level of residual risk. This risk should be documented and, if necessary, escalated to senior leadership for further review or acceptance.

4.5 Ongoing Risk Assessment

Risk assessments should not be considered a one-time event. Instead, they should be ongoing and adaptive to changes in the environment. Departments and system owners are required to:

- Conduct Regular Risk Assessments: Risk assessments must be conducted at least annually for all critical systems and more frequently for systems handling Confidential Data or those subject to regulatory requirements. Assessments should also be triggered by major system changes, such as software upgrades, system migrations, or significant business process changes.
- Respond to Emerging Threats: As new threats and vulnerabilities emerge, system owners must perform ad-hoc assessments to identify potential impacts. This proactive approach ensures that the organization remains resilient to evolving risks.
- Risk Assessment Tools: Use automated tools and services provided by the Information Security Office to aid in the identification and management of risks. These tools can streamline the assessment process and provide insights into system vulnerabilities.

4.6 Reporting

The results of each risk assessment must be documented and reported to the Information Security Office. Reports should include:

- A summary of identified risks, their likelihood and impact scores, and the calculated risk levels.
- Mitigation plans for high and critical risks, including timelines and responsible parties.
- Any residual risks that remain after mitigation efforts.
- A plan for ongoing monitoring and the timeline for the next assessment.

Risk reports will be reviewed by the CIO and Information Security Office to ensure alignment with the organization's overall risk posture and strategic priorities.

5. Risk Mitigation and Control

This section outlines the actions to be taken once risks are identified, emphasizing the implementation of appropriate security controls.

Once risks have been assessed and prioritized, system owners must develop a risk mitigation plan that outlines specific controls to reduce or eliminate the risk. Controls may include technical solutions, such as software patches or encryption, process improvements, or changes in user access levels.

Risk mitigation plans should be aligned with industry best practices and regulatory standards where applicable. High-priority risks, particularly those that could result in the compromise of confidential data or critical systems, must be addressed immediately. Lower-priority risks should be managed according to their severity and potential impact on operations.

Departments are responsible for documenting all mitigation strategies and regularly reviewing the effectiveness of implemented controls. Any unmitigated risks must be escalated to the CIO and senior leadership for further evaluation.

6. Monitoring and Reporting

This section provides guidance on ongoing risk monitoring and the reporting mechanisms necessary for maintaining accountability.

The risk management process does not end with mitigation. Departments and system owners must continuously monitor their systems for new or emerging risks. This includes regularly reviewing security logs, conducting vulnerability scans, and reassessing risks based on changes in technology, processes, or the threat landscape.

The Information Security Office will conduct periodic audits to ensure compliance with the organization's risk management policy. Departments must submit regular reports on their risk assessment activities, including the status of mitigation efforts and any unresolved risks. These reports will be reviewed by the CIO and senior management to ensure ongoing risk management alignment with organizational goals.

7. Enforcement

This section explains how compliance with the Risk Management Policy is enforced and the consequences of non-compliance.

Compliance with the Risk Management Policy is mandatory for all departments, system owners, and IT professionals. Failure to conduct regular risk assessments or implement appropriate mitigation measures may result in disciplinary actions, including formal warnings, loss of access to information systems, or termination of employment or contracts.

The Information Security Office will audit compliance with this policy on a regular basis. Non-compliance will be documented, and corrective actions will be enforced. Severe violations may result in escalation to senior management, external audits, or legal action if non-compliance leads to significant security incidents or regulatory breaches.