COLLEGE POLICY: 468

INFORMATION TECHNOLOGY RISK MANAGEMENT

PURPOSE

Risk management is a critical component of any information security program. It helps ensure that any risk to confidentiality, integrity, and availability is identified, analyzed, and maintained at acceptable levels. Risk assessments allow management to prioritize and focus on areas that pose the greatest impact to critical and sensitive information assets. This provides the foundation for informed decision-making regarding information security.

Federal and State mandates require routine assessments to identify risk and ensure appropriate controls. Risk assessments allow alignment of information security with business objectives and regulatory requirements. Identifying information security risk and considering control requirements from the onset is essential, and far less costly than retrofitting or addressing the impact of a security incident.

The National Institute of Standards and Technology (NIST) provides a risk management framework to evaluate current security posture, identify gaps, and determine appropriate actions.

SCOPE

This policy applies to all college information technology and information management systems to address enterprise and system risk. All information systems (including outsourced IT services) shall undergo some level of assessment of information security risk management. Information systems deemed to be of critical value to the college, including but not limited to IT systems where formal project management is required, shall undergo formal risk management activities as defined in this Policy.

RESPONSIBILITY AND AUTHORITY

Campus management is responsible for the oversight, implementation, and monitoring of risk management. All polices and procedures related to risk management practices are subject to approval by the Chancellor's Cabinet, Board of Visitors, and UA System Board of Trustee's.

The Director of Information Technology will ensure the risk management process is established and maintained. Information Technology staff will continuously monitor risks and update procedural controls as needed.

POLICY

Information security risk management considers vulnerabilities, threat sources, and security controls that are planned or in place. These inputs are used to determine the resulting level of risk posed to information, systems, processes, and individuals that support business functions.

Any system or process that supports business functions must be appropriately managed for risk and undergo risk assessments as part of its life cycle.

1. Security Categorization

    a. Appropriate security controls will be applied to data categorized as confidential/sensitive, including any personally identifiable information (PII) and protected health information (PHI), in accordance with state and federal laws, directives, policies, regulations, and standards.

    b. Document the security controls (including supporting rationale) in the information security plan for the information system.

2. Risk Assessment

    a. Conduct (or have conducted by a qualified third-party) an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.

    b. Update, review, and document changes to risk assessment results as needed. Update whenever there are significant changes to the system or operating environment.

3. Vulnerability Scanning

    a. Conduct (or have conducted by a qualified third-party) a scan for vulnerabilities in the information system and hosted applications annually and/or randomly when new vulnerabilities potentially affecting the system/applications are identified and reported.

    b. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
        i. Software flaws and improper configurations.
        ii. Measuring vulnerability impact.

    c. Analyze vulnerability scan reports and results from security control assessments.

    d. Remediate legitimate vulnerabilities within one month in accordance with an organization assessment of risk.

4. Penetration Testing

    a. Conduct (or have conducted by a qualified third-party) a network penetration test on all systems.

b. Remediate any findings from the penetration test.

5. Training

a. UA Cossatot will provide periodic training to relevant individuals on the applicable provisions of this policy. The purpose of this training is to ensure that Risk Management personnel maintain a current understanding of the universe of threats creating risks in need of control, techniques for measuring inherent and residual risk, and which risks are addressed by a given control.

Policy History:
May 2, 2022

INFORMATION TECHNOLOGY RISK MANAGEMENT

Procedures/Guidelines

1. Risk Analysis Methodology: Each risk analysis or assessment conducted by, or at the direction of, the IT Risk Governance Committee should adhere to the following base methodology:

    a. Identify the Scope of the Analysis: The scope of any risk analysis or assessment encompasses the potential risks and vulnerabilities to the confidentiality, availability, and integrity of sensitive data that the college creates, receives, maintains, or transmits electronically. For each individual risk analysis or assessment, IT will define the information assets that will comprise the scope of the risk analysis or assessment, which will include, at a minimum, systems, applications, and devices that create, receive, maintain, or transmit sensitive data.

    b. Gather Data: Gather relevant data by reviewing past and/or existing projects, performing interviews, reviewing documentation, or using other data gathering techniques. Document data gathering activities and data gathered to be included as part of the risk analysis results.

    c. Identify and Document Potential Threats and Vulnerabilities: Identify and document potential threats and vulnerabilities to the confidentiality, availability, and integrity of information assets. Identified threats should include possible threat vectors including people, process and technology.

    d. Assess Current Security Measures: Analyze current control activities implemented to minimize or eliminate risks. Document analysis, including whether requisite security measures are in place, and if current security measures are configured and used properly. This process may include recent audit testing results, updated technical scans, and control effectiveness observation.

    e. Determine Likelihood of Threat Occurrence: Establish the probability (likelihood) that an identified threat will trigger or exploit a specific vulnerability. Ratings such as high, medium, and low or numeric representations of probability may be used to express the likelihood of occurrence.

    f. Determine the Potential Impact of Threat Occurrence: Determine the potential impact of identified threats triggering or exploiting a specific vulnerability. Such impact may be expressed using quantitative, semi-quantitative or qualitative metrics, but should convey the potential impact to the college.

    g. Determine the Level of Risk: Determine the level of risk by analyzing the values assigned to the likelihood of threat occurrence and the resulting impact of threat

occurrence. Document each assigned risk level, including a list of corrective actions to be performed to mitigate each risk level.

h. Identify Security Measures and Finalize Documentation: Identify security measures that can be used to reduce risk to a reasonable and appropriate level and conduct cost/benefit analysis to determine appropriate, effective, and efficient controls. Generate a risk analysis report that documents the risk analysis process, output of each step and initial identification of security measures.

2. Evaluation

a. UA Cossatot shall perform evaluations directly or engage the services of a third party to conduct on behalf of the college. Evaluations may include a review of policies and procedures to evaluate their appropriateness and effectiveness in protecting against reasonably anticipated threats, a gap analysis, an assessment of security controls, and testing and evaluation to determine whether controls have been implemented properly. Following each evaluation, the Health System shall update its security policies, procedures, controls, and processes, as appropriate, based on the results of the evaluation.

Procedure History:
April 21, 2022