IT Risk & Data Classification

The University of Nebraska is committed to protecting the confidentiality, integrity, and availability of information important to the University's mission. Executive Memorandum No. 42 – Policy on Risk Classification and Minimum-Security Standards establishes risk classifications for University of Nebraska data and information systems. University data and information systems are required to be classified into one of the following categories: Low Risk, Medium Risk, or High Risk. Each risk classification is paired with corresponding Minimum-Security Standards that align to National Institute of Standards and Technology (NIST) frameworks. Some data may also be classified by agreement or regulation requiring additional compliance requirements.

What is Risk?

Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Importance of Determining IT Risk

Determining information security risk enables the university to implement the appropriate security controls to balance usability and defensibility of information systems and data. When risk is accounted for, the University can minimize inherent risks by appropriately managing confidentiality, integrity, and availability of information systems to match the University's' risk appetite.

What is an IT Risk Assessment?

A risk assessment is the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Risk Assessments are made up of several components:

- Threat Event Assessment
- Likelihood of Occurrence
- Impact of Occurrence
- Overall Risk Assessment Summarization.

Threat events are analyzed for the likelihood of occurrence and the impact while considering existing mitigations and controls. The risk assessment supplies the information needed to manage risk properly and effectively by supplying a summarization of the risk, recommendations for new mitigations to reduce the risk, and risk score for the information system or data.

What is IT Risk Management?

Risk management is the process for prioritizing and addressing the risks identified during the assessment process over time. Risk management balances recommended mitigations with financial constraints, usability, and organizational priorities according to the University's risk appetite. For questions or consultation, please reach out to its-sec-compliance@nebraska.edu

Definitions

Availability
Ensuring timely and reliable access to and use of information.

Confidentiality
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Impact Level
The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Inherent Risk
Portion of risk without security measures applied.

Integrity
Improper information modification or destruction and includes ensuring information non-repudiation and authenticity.

Likelihood of Occurrence
The probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.

Residual Risk
Portion of risk remaining after security measures have been applied.

Risk Appetite
The amount of risk an organization is willing to accept.

Threat
Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

Threat Event Assessment
Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.

Resources – May be found at: https://its.nebraska.edu/it-risk-classification

- Executive Memorandum 42 – Policy on Risk Classification and Minimum-Security Standards
- ITS-13: Risk Management Standard
- ITS Risk Classification Page
- Risk Classification Self-Assessment
- NIST 800-30r1 – Guide for Conducting Risk Assessments