NCSA Risk Management Program

Document Name: NCSA Risk Management Program
Version: 1.1
Accountable: Alex Withers
Authors: Alex Withers

Reviewed: June 23, 2021
Approved: Dec 20, 2019

Purpose

Risk Management Program to conduct thorough and timely risk assessments of the potential threats and vulnerabilities to the confidentiality, integrity, and availability of NCSA's computational resources. This program enables NCSA to develop strategies to efficiently and effectively mitigate the risks identified in the assessment process. Information produced during the risk assessment will be used to determine and manage security controls for NCSA's computational resources.

Scope

This risk management program applies to all NCSA resources that do not fall under a separate risk management program (i.e. ACHE).

Standards

The risk management program consists of two processes:

1. **Risk Assessment** - Identifies and prioritizes the risks to information system security and determines the probability of occurrence and the resulting impact for each threat/vulnerability pair identified given the security controls in place.
2. **Risk Mitigation** - a process that prioritizes, evaluates, and implements security controls that will reduce or offset the risks determining the risk assessment process to satisfactory levels within an organization given its mission and available resources.

Risk Assessment Frequency

A risk assessment will be performed periodically by the NCSA Security Office. Exceptions to this include (i) substantial infrastructure/environment changes that would require a new impact analysis and (ii) a security incident that warrants reevaluation of risks.

Risk Assessment Components

A risk assessment is conducted as per the documented **NCSA Risk Assessment and Mitigation** procedure. Risks will be recorded in the NCSA risks register, and risk assessments will be saved indefinitely.

NCSA implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:

1. Ensure the confidentiality, integrity, and availability of all NCSA computational resources and
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of NCSA's data.

Risk Management Process

The risk assessment is part of an on-going process to understand and manage risk. The broader process contains the following steps as per the documented **NCSA Risk Assessment and Mitigation** procedure:

- A risk assessment performed.
- Findings are submitted to the NCSA Security Office within 30 days, and the Security Office forwards it to senior management.
- The NCSA Security Office works with the project(s) to remediate vulnerabilities and mitigate risks within 90 days of finishing the assessment. If this is not possible for all risks, an exemption must be requested in writing to the Security Office.
- Remediation activities are documented in a remediation plan.
- The remediation plan is sent to the Security Office, who sends it to senior management.

Privacy

All data from the risk assessment is kept confidential and not shared without written approval from the NCSA Security Office.

Consequences

All workforce members are expected to fully cooperate with all persons charged with doing risk management work.