NCSA Risk Assessment and Mitigation

Document Name: NCSA Risk Assessment and Mitigation
Version: 1.2
Accountable: Alex Withers
Authors: Alex Withers

Reviewed: June 23, 2021
Approved: Nov 1, 2019

Purpose

The intent of completing a risk assessment is to determine potential threats and vulnerabilities and the likelihood and impact should they occur. The output of this process helps to identify appropriate controls for reducing or eliminating risk.

Scope

This process of risk assessment and mitigation applies to any NCSA resources that are required to undergo a risk assessment. ***Note that the outputs below are compatible with NCSA's risk register in its MIS system.***

Risk Assessment

1. ***System Characterization*** - The first step in assessing risk is to define the scope of the effort. Concretely define the boundaries of the system(s) that you are evaluating. For ACHE, identify systems where sensitive data including ePHI and CUI is created, received, maintained, processed, or transmitted. ***Output*** – Characterization of the IT system assessed, a good picture of the IT system environment, and delineation of system boundaries.
2. ***Threat Identification*** - In this step, potential threats (the potential for threat-sources to successfully exercise a particular vulnerability) are identified and documented. Consider all potential threat-sources through the review of historical incidents and data from intelligence agencies, the government, etc., to help generate a list of potential threats. ***Output*** – A threat statement containing a list of threat-sources that could exploit system vulnerabilities.
3. ***Vulnerability Identification*** - The goal of this step is to develop a list of technical and non-technical system vulnerabilities (flaws or weaknesses) that could be exploited or triggered by the potential threat-sources. Vulnerabilities can range from incomplete or conflicting policies that govern an organization's computer usage to insufficient safeguards to protect facilities that house computer equipment to any number of software, hardware, or other deficiencies that comprise an organization's computer network. ***Output*** – A list of the system vulnerabilities (observations) that could be exercised by the potential threat-sources.
4. ***Control Analysis*** - The goal of this step is to document and assess the effectiveness of technical and non-technical controls that have been or will be implemented by the organization to minimize or eliminate the likelihood (or probability) of a threat-source exploiting a system vulnerability. ***Output*** – List of current or planned controls (policies, procedures, training, technical mechanisms, insurance, etc.) used for the IT system to mitigate the likelihood of a vulnerability being exercised and reduce the impact of such an adverse event.
5. ***Likelihood Determination*** - The goal of this step is to determine the overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat-source given the existing or planned security controls. ***Output*** – Likelihood rating of low (1), medium (3), or high (5). Refer to the NIST SP 800-30 definitions of low, medium, and high.
6. ***Impact Analysis*** - The goal of this step is to determine the level of adverse impact that would result from a threat successfully exploiting a vulnerability. Factors of the data and systems to consider should include the importance to the organization's mission; sensitivity and criticality (value or importance); costs associated; loss of confidentiality, integrity, and availability of systems and data. ***Output*** – Magnitude of impact rating of low (1), medium (3), or high (5). Refer to the NIST SP 800-30 definitions of low, medium, and high.
7. ***Risk Determination*** - This step is intended to establish a risk level. By multiplying the ratings from the likelihood determination and impact analysis, a risk level is determined. This represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. ***Output*** – Risk level of low (1-8), medium (9-17) or high (18-25). Refer to the NIST SP 800-30 definitions of low, medium, and high.
8. ***Control Recommendations*** - The purpose of this step is to identify controls that could reduce or eliminate the identified risks, as appropriate to the organization's operations to an acceptable level. Factors to consider when developing controls may include effectiveness of recommended options (i.e., system compatibility), legislation and regulation, organizational policy, operational impact, and safety and reliability. Control recommendations provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented. ***Output*** – Recommendation of control(s) and alternative solutions to mitigate risk.

1. ***Results Documentation*** - Results of the risk assessment are documented in an official report or briefing and provided to senior management to make decisions on policy, procedure, budget, and system operational and management changes. ***Output*** – A risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation.

Risk Mitigation

Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process to ensure the confidentiality, integrity and availability of NCSA's computational resources (and specifically ePHI and CUI for the ACHE). Determination of appropriate controls to reduce risk is dependent upon the risk tolerance of the organization consistent with its goals and mission.

1. ***Prioritize Actions*** – Using the results from Step 7 of the Risk Assessment, sort the threat and vulnerability pairs according to their risk-levels in descending order. This establishes a prioritized list of actions needing to be taken, with the pairs at the top of the list getting/requiring the most immediate attention and top priority in allocating resources. ***Output*** – Actions ranked from high to low
2. ***Evaluate Recommended Control Options*** – Although possible controls for each threat and vulnerability pair are arrived at in Step 8 of the Risk Assessment, review the recommended control(s) and alternative solutions for reasonableness and appropriateness. The feasibility (e.g., compatibility, user acceptance, etc.) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended controls should be analyzed. In the end, select a "most appropriate" control option for each threat and vulnerability pair. ***Output*** – list of feasible controls
3. ***Conduct Cost-Benefit Analysis*** – Determine the extent to which a control is cost-effective. Compare the benefit (e.g., risk reduction) of applying a control with its subsequent cost of application. Controls that are not cost-effective are also identified during this step. Analyzing each control or set of controls in this manner, and prioritizing across all controls being considered, can greatly aid in the decision-making process. ***Output*** – Documented cost- benefit analysis of either implementing or not implementing each specific control.
4. **Select Control(s)** – Taking into account the information and results from previous steps, NCSA's mission, and other important criteria, the Risk Management Team determines the best control(s) for reducing risks to the information systems and to the confidentiality, integrity, and availability of NCSA's computational resources (and specifically ePHI and CUI for the ACHE). These controls may consist of a mix of administrative, physical, and/or technical safeguards. **Output** – Selected control(s) .
5. ***Assign Responsibility*** – Identify the individual(s) or team with the skills necessary to implement each of the specific controls outlined in the previous step, and assign their responsibilities. Also identify the equipment, training and other resources needed for the successful implementation of controls. Resources may include time, money, equipment, etc. ***Output*** – List of resources, responsible persons and their assignments
6. **Develop Safeguard Implementation Plan** –
    a. Develop an overall implementation or action plan and individual project plans needed to implement the safeguards and controls identified. The Implementation Plan should contain the following information:
        i. Each risk or vulnerability/threat pair and risk level
        ii. Prioritized actions
        iii. The recommended feasible control(s) for each identified risk
        iv. Required resources for implementation of selected controls
        v. Team member responsible for implementation of each control
        vi. Start date for implementation
        vii. Target date for completion of implementation
        viii. Maintenance requirements.
    b. The overall implementation plan provides a broad overview of the safeguard implementation, identifying important milestones and timeframes, resource requirements (staff and other individuals' time, budget, etc.), interrelationships between projects, and any other relevant information. Regular status reporting of the plan, along with key metrics and success indicators should be reported to the organization's executive management/leadership team (e.g. the Board, senior management, and other key stakeholders).
    c. Individual project plans for safeguard implementation may be developed and contain detailed steps that resources assigned to carry out to meet implementation timeframes and expectations (often referred to as a work breakdown structure). Additionally, consider including items in individual project plans such as a project scope, a list of deliverables, key assumptions, objectives, task completion dates and project requirements.
    d. **Output** – Safeguard Implementation Plan
7. ***Implement Selected Controls*** – as controls are implemented, monitor the affected system(s) to verify that the implemented controls continue to meet expectations. Elimination of all risk is not practical. Depending on individual situations, implemented controls may lower a risk level but not completely eliminate the risk.
    a. Continually and consistently communicate expectations to all Risk Management Team members, as well as senior management and other key people throughout the risk mitigation process. Identify when new risks are identified and when controls lower or offset risk rather than eliminate it.
    b. Additional monitoring is especially crucial during times of major environmental changes, organizational or process changes, or major facilities changes.
    c. If risk reduction expectations are not met, then repeat all or a part of the risk management process so that additional controls needed to lower risk to an acceptable level can be identified.
    d. **Output** – Residual Risk