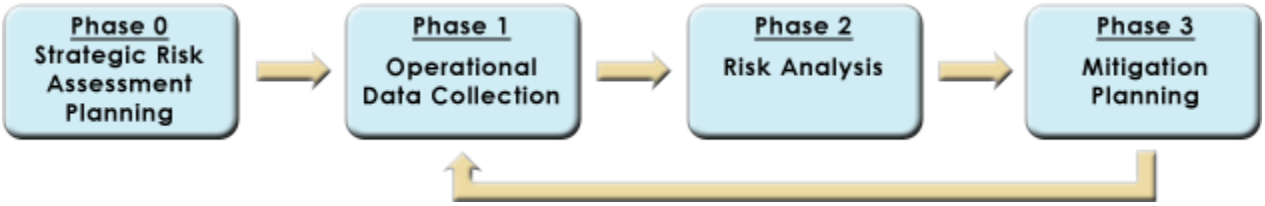
Risk Management Framework

Risk Management Framework

Version 2.0 -- October 2008 (see comment below for more information)



Purpose:
The Higher Education Information Security Council (HEISC) risk assessment / management framework is intended to provide high-level guidance for an effective cyber-risk assessment and management process for institutions of higher education. It is intended to provide a model process which can be adapted, as needed, for any institution regardless of size, funding model, or culture.

Background and overview:
In virtually every aspect of education, research, and administration there is an increased reliance on digital information and the technologies that support it. With this comes an increasing level of responsibility to protect these information assets from accidental or malicious exposure or damage. In light of current and pending federal and state legislation, it is imperative for universities to recognize that information risk management must be part of their strategic and continuity planning.

Risk management is the ongoing process of identifying these risks and implementing plans to address them. Risk is determined by considering the likelihood that known threats will exploit vulnerabilities and the impact they have on valuable assets. Sometimes risk is expressed as a conceptual formula: _ Risk_ = *Threat* x *Vulnerability* x *Impact.*

Risk assessment is the part of the ongoing risk management process that assigns relative priorities for mitigation plans and implementation. It is a large part of the overall risk management process; many of the steps described in this framework focus on the assessment process.

Risk decisions are made all the time, sometimes without deep consideration and may even be based upon intuition. A formalized risk management process can uncover risks that were not anticipated, resolve funding conflicts, and help enhance executive buy-in to security improvements.

> Some risk terms might be confusing. A ***vulnerability assessment*** is basically an inventory of all vulnerabilities. It is often thought of as just a technical examination (networks scanning, etc) but a complete vulnerability assessment would include all manner of vulnerabilities - physical, process, etc. The ***risk assessment*** considers those vulnerabilities in light of the other aspects of the risk formula - threats and impact (which includes the concepts of both asset and value) so that the potential mitigations that might be applied can be prioritized. ***Risk management*** is actually doing all that plus actually mitigating the selected vulnerabilities, measuring the outcome of the process, and repeating the process again and again. Often, the number of assets potentially at risk exceeds the resources available to manage them. It is therefore extremely important to know where to apply available resources to mitigate the highest priority risks in an efficient and cost-effective manner. It is also important to balance security with usability.

Using the Framework:
Risk assessment and management scope may vary. For instance, assessments may be conducted as part of the planning and purchasing process for significant projects or systems. Assessments may also be conducted in response to IT security incidents to help ensure incidents do not recur. They may also be conducted on some regular, periodic basis to assure ongoing compliance and up-to-date security measures.

Moreover, institutions vary in many ways including size, complexity, classification, culture, private/public, and so on. The depth and focus of assessments conducted will often depend upon these and other local considerations. While it is certainly possible to follow every step in every process in every phase of this framework (and many institutions do so) the intent of the framework is to be adaptable to local requirements. It is expected that institutions may decide to combine certain steps or processes to streamline the framework for specific purposes.

Especially for comprehensive risk assessments at large institutions, depth might need to be balanced with feasibility to complete the assessment in a reasonable time frame. Resisting the urge to be overly comprehensive is important because assessments that take longer than a few months to complete may lose value as data becomes stale. Here are some tips to help manage large comprehensive assessments.

- Aggregate resources into similar groups and assess the group rather than individual resources. For example, rather than assess each workstation, aggregate similar workstations in to a group and assess them as a group.
- Avoid straying from the process. Resist mission creep.
- Focus on most critical assets
    - The most confidential IT resources
    - IT resources with highest availability requirements
    - IT resources with the most strict integrity requirements
    - IT resources that are critical to the mission and function of the unit
    - IT resources that are most difficult to replace
    - IT resources that are most expensive to replace

Regardless of the assessment scope or local modifications to the process, all four phases of this framework will always apply.

Other points to consider:

1. Risk assessment should be thought of as an ongoing process, not as a one-time project. The process is described as a set of steps that are continually repeated. At the outset, however, there is a start-up process that usually is not repeated.
2. Conducting a university-wide information risk assessment is a process that will require strong commitment from upper administration and collaboration between cross-functional units. Assessing information risks is a management issue, not a technology issue; therefore, to be most effective, the process should be considered the responsibility of all members of management. An effective university information risk assessment needs to become a part of the culture of the university community, involving not only IT-staff but also all key staff, administrators, faculty, and students. Education and awareness efforts should be aimed at all of these constituencies.
3. Due to the complexities of a university environment, a university-wide information risk assessment requires planning and, more importantly, a strategy that systematically increases the scope of the information risk assessment until it encompasses all university areas.
4. A sound risk management program can serve as the basis for prioritizing and resolving possible funding conflicts.

Top of page

Phase 0: Strategic Risk Assessment Planning (a one-time process)

Goals: Establish the strategy for assessing risk. Determine the criteria that will be used to evaluate the strategic importance of assets (often called "asset classification" - please see the Data Classification Toolkit for more comprehensive information on this topic), threats and vulnerabilities.

Note: Although nothing in this phase is generally repeated, it is possible at any time in the ongoing risk assessment process to either research or discover an additional useful criterion or specific question to be answered and add it to the set already in use.

Process 1: Establish Criteria that will be used to Classify and Rank Data Assets

Steps

1. Decide on the number of data asset risk criticality levels to establish.
2. Starting only with what is already known about the institution, determine the risk assessment criteria for identifying critical data asset levels (see Risk Assessment Matrix Example for a starter set suitable for most institutions of higher education).

Process 2: Apply Classification Criteria to Rank Data Assets and Related IT Resources

Steps

1. Classify institutional files, databases, tables, and other data collections according to the highest level of critical asset it contains.
2. Classify other related information resources (e.g., information systems, servers, network segments, desktop computers, off-line storage facilities) according to the level of risk criticality already assigned to the data asset.

Process 3: Identify Threats, Vulnerabilities and Controls that will be Evaluated

Steps

1. Establish a system for identifying asset threats.
2. Establish a system for identifying asset vulnerabilities and controls.

Process 4: Establish Criteria that will be used to Evaluate Threats, Vulnerabilities and Controls

Steps

1. Determine the criteria to establish for evaluating threat probability and impact.
2. Determine the criteria to establish for evaluating vulnerabilities and controls.

Top of page

Phase 1: Operational Data Collection

Goals: Identify and prioritize the institution's critical assets. Identify key threats and vulnerabilities that could compromise the confidentiality, integrity and availability of these assets. Identify all protection in place to safeguard these assets and which vulnerabilities and threats they impact.

Note: It is important that all levels of the institution participate in this phase in order to derive an accurate perspective of the institution's security posture. Senior management provides the overall vision and feedback on the organization's "appetite" for risk. Technical staff is best suited to comment on the infrastructure and third party applications. Users provide valuable insight by characterizing their knowledge and awareness of appropriate behavior to protect the institution's assets.

Process 1: Strategic Perspective - Senior Management

Steps

1. Identify senior management to include in the risk assessment initiative.
2. Obtain senior management "buy-in"to the project.
3. Understand the institution's strategic view.

Process 2: Operational Perspective: Infrastructure - Technical staff

Steps

1. Identify IT staff to include in the risk assessment.
2. Obtain the technical staff's perspective on asset vulnerabilities, threats and controls.

Process 3: Operational Perspective: Applications - General staff

Steps

1. Identify key staff to survey for operational perspective.
2. Obtain the staff perspective on asset vulnerabilities, threats and controls.

Process 4: Technical Perspective - Technical Evaluation

Steps

1. Identify key technology components of critical assets for technical evaluation.
2. Determine evaluation approach.
3. Run evaluation tool(s) on selected technology components.
4. Summarize results.

Top of page

Phase 2: Risk Analysis

Goals: In this phase, risk profiles are created for threats that are most likely to have the largest impact on asset vulnerabilities. This information may then be used to prioritize the cost-effective allocation of resources to ensure appropriate mitigation of the highest risks, balancing usability with security.

Process 1: Review Documentation and Technical Data

Steps

1. Review policies, reports, documentation and diagrams to determine if they are current, adequate and accurate.
2. Analyze the results of the technical evaluation.

Process 2: Consolidate and Prioritize Perspectives

Steps

1. Identify risks.
2. Create profiles that show a consolidated view of each risk.
3. For each risk profile, compose a risk statement.

Top of page

Phase 3: Mitigation Planning

Goals: Finally, the protection strategy to mitigate risk is documented. Using the risk statements created in Phase 2, determine which risks will be addressed in the final mitigation strategy. This is also a good time to evaluate the effectiveness of the risk assessment process and begin planning the next assessment with consideration for lessons learned in the current assessment.

Process 1: Agree on a Strategy to Mitigate Risks

Steps

1. Develop options to mitigate risk.
2. Confer with management to agree upon the best mitigation strategies for the institution.

Process 2: Document and Implement Mitigation Plan

Steps

1. Develop specific action plans to mitigate risks.

2. Establish metrics to evaluate progress and success.
3. Compile final mitigation report for management.

Process 3: Evaluate Mitigation Progress and Plan Next Assessment

Steps

1. Evaluate mitigation progress and success.
2. Document improvements to risk assessment procedures.
3. Plan the next risk assessment.

Top of page
