

**RISK ASSESSMENT WORKING GROUP**  
**EDUCAUSE/Internet2 Security Task Force**  
**Risk Assessment Framework**

**Purpose:**

To provide a high-level overview on the subject of conducting a risk assessment of information systems within higher education.

**Background and overview:**

There is an increased reliance on digital information and the technologies that support it in virtually every aspect of the educational, research, and administrative processes of higher education, which has brought with it an increasing level of responsibility to protect these information assets from accidental or malicious exposure or damage. ***Risk management*** is the ongoing process of identifying these risks and implementing plans to address them.

Often, the number of assets potentially at risk outweighs the resources available to manage them. It is therefore extremely important to know where to apply available resources to mitigate risk in a cost-effective and efficient manner. ***Risk assessment*** is the part of the ongoing risk management process that assigns relative priorities for mitigation plans and implementation.

**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 startup 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.
3. 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 planning.
4. 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.
5. 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 staff, administrators, faculty, and students. Education and awareness efforts should be aimed at all of these constituencies.

6. Effective risk management practices require a “risk aware” culture: universities need to expand their information security training and awareness programs to emphasize the importance of adopting risk management principles.
7. A sound risk management program can serve as the basis for prioritizing and resolving possible funding conflicts.

### **Phase 0: Establish Risk Assessment Criteria for the Identification and Prioritization of Critical Assets** (a one-time process)

**Goals:** to quickly establish the overall criteria for the identification of critical data assets and their appropriate priority level and to obtain senior management’s perspective on issues of strategic importance.

#### **Process 1: Establish Risk Assessment Criteria**

##### Steps

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

*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 2: Apply the Critical Asset Criteria to Classify Data Collections and Related 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, offline storage facilities) according to the level of risk criticality already assigned to the data asset.

## **Phase 1: Develop Initial Security Strategies**

**Goals:** Once the information assets have been classified, strategic planning for the rest of the risk management process can begin. Vulnerabilities can be identified, and the process of mitigating the threats that can exploit those vulnerabilities can begin. An institution can decide to specifically focus on the very highest risks, or it may decide to focus first on mitigating risks broadly (or both). The mere process of bringing management together to discuss the organization's strategy about risk mitigation can be extremely fruitful

### **Process 1: Strategic Perspective—Senior Management**

#### Steps

1. Identify senior management to interview and to include in the process, making sure to include key stakeholders in administrative, academic, and research components.
2. Use the ISG Assessment Tool as a planning guide to understand senior management's priorities and areas of concern as well as management's "risk appetite" (the degree of risk that management will be willing to accept without applying further resources to mitigate the risk)

### **Process 2: Operational Perspective—Departmental Management**

#### Steps

1. Identify a representative group of departmental management to interview (including management of mission-critical areas)
2. Discuss their views on critical assets and relative priorities
3. Identify areas of risk
4. Identify security requirements for the most important assets

### **Process 3: Practice Perspective—Staff**

#### Steps

1. Identify representative staff within these mission-critical areas to interview
2. Discuss their views on critical assets and relative priorities
3. Identify areas of risks
4. Identify security requirements for the most important assets
5. Capture knowledge of current security practices and organizational vulnerabilities

## **Process 4: Consolidated View of Security Requirements**

### Steps

1. Select critical assets
2. Refine and prioritize security requirements for critical assets (availability, confidentiality, integrity)
3. Identify current protection strategies for critical assets (include an evaluation of the resources currently applied to mitigate the risks and estimate the additional resources that might need to be applied to enhance the risk management process)

## **Phase 2: Technological View—Identify Infrastructure Vulnerabilities**

**Goals:** To identify areas of potential exposure associated with the systems architecture.

## **Process 5: Key Technology Components**

### Steps

1. With management, identify all systems associated with critical assets
2. Identify key technology components for each critical asset and system; consider servers, networking components, security components, desktops, home computers, laptops, storage devices, wireless components, etc.)
3. Select specific technology components for evaluation
4. Decide on the evaluation approach (tools: O/S scanners, network scanners, scripts, checklists, etc.)

## **Process 6: Selected Technology Components Evaluation**

### Steps

1. Coordinating with management, run vulnerability evaluation tools on selected infrastructure components
2. Review technology vulnerabilities and summarize results

## **Phase 3: Risk Analysis—Develop Security Strategy and Plans**

**Goals:** After identifying key information systems resources and evaluating the degree of vulnerability with the systems, quantitatively determine the level of risk associated with each system and system component. This information may then be used to prioritize the allocation of resources to ensure appropriate mitigation of the highest risks and to make appropriate management decisions about the degree of risk that the organization will be willing to accept.

## **Process 7: Risk Assessment**

### Steps

1. Assess the potential impact of threats (and vulnerabilities) to critical assets (qualitative and/or quantitative)
2. Evaluate the likelihood of occurrence of the threats (high, medium, low)
3. Create a consolidated analysis of risks, based on the impact value to critical assets and the likelihood of occurrence

## **Process 8: Protection Strategy and Mitigation Plans**

### Steps

1. Develop strategies for improving the organizations security-related practices
2. Develop risk mitigation plans to cost-effectively reduce risks to critical assets
3. Develop specific action plans to improve security practices and to mitigate risks to critical assets, taking into consideration the cost-benefit and the organization's risk appetite

### **Summary**

It is important to note that this is a process that has no finish line. While a risk assessment—the process of identifying and quantifying risks—might take place on an infrequent basis (e.g., annually), the risk management process—the ongoing process of mitigating the risks to the organization—should be ingrained into the institution's culture to be most effective.

## Appendix A: Starter Set of Risk Assessment Criteria for Identifying Critical Data Assets

This starter set is usually found to be sufficient for most institutions of higher education. However, any institution can choose to add to, subtract from, or otherwise modify the number of levels selected or the specific risk assessment criteria outlined here.

|                                  | <b>Most Critical</b><br><i>Highest level of sensitivity</i>   | <b>Critical</b><br><i>Moderate level of sensitivity</i>  | <b>Least Critical</b><br><i>Very low, but still requiring some protection</i>   |
|----------------------------------|---|--|---|
| <b>Legal Requirements</b>        | Protection of data is required by law (e.g., HIPAA and FERPA data elements and other personal identifying information protected by law)   | The institution has a contractual obligation to protect the data (e.g., bibliographic citation data, bulk licensed software)   |   |
| <b>Reputation Risk</b>           | High  | Medium   | Low   |
| <b>Other Institutional Risks</b> | Information that provides access to resources, physical or virtual  | Smaller subsets of Most Critical data from a school, large part of a school, or department   |   |
| <b>Data Examples</b>             | <ul style="list-style-type: none"> <li>• Medical</li> <li>• Student</li> <li>• Prospective student</li> <li>• Personnel</li> <li>• Donor or prospect</li> <li>• Financial</li> <li>• Contracts</li> <li>• Physical plant detail</li> <li>• Credit card numbers</li> <li>• Certain management information</li> </ul> | <ul style="list-style-type: none"> <li>• Information resources with access to Most Critical data</li> <li>• Research detail or results that are not Most Critical</li> <li>• Library transactions (e.g., catalog, circulation, acquisitions)</li> <li>• Financial transactions that do not include Most Critical data (e.g., telephone billing)</li> <li>• Very small subsets of Most Critical data</li> </ul> | <ul style="list-style-type: none"> <li>• Campus maps</li> <li>• Personal directory data (e.g., contact information)</li> <li>• E-mail</li> <li>• Institutionally published public data</li> </ul> |