Risk Management

Table of Contents

Getting Started

Developing an effective risk management program is important in building an information security program. Risk management activities should take into account **people, business processes (information handling), and technology**.

Evaluate and select risk management methods:

- **ISO/IEC 27005:2011** provides guidance in establishing a risk management program, and describes how to implement each phase of risk management (identification, assessment, treatment, monitoring and review)
- **NIST Special Publication 800-39**, Managing Information Security Risk: Organization, Mission and Information System View, describes the fundamentals and the process of completing risk assessments
- **NIST Special Publication 800-30 Revision 1** is a Guide For Conducting Risk Assessments
- **ISO/IEC 27002:2013** is an international standard that assists organizations with evaluating information security controls and performing risk treatment activities
- **NIST Special Publication 800-37 Revision 1**, Guide for Applying the Risk Management Framework, offers guidance in evaluating controls and applying risk treatment methods
- The **HEISC Risk Management Framework** is closely aligned with the guidance provided in the NIST publications cited above
- **ISO/IEC 27005:2011**, used in combination with the above framework, provide a complementary and comprehensive approach to identifying, assessing, and treating risks

Perform a high level risk assessment:

1. **Identify** risks associated with information handling/business processes and begin educating the stakeholder community about information security risk management and what's involved in various stages (risk identification, assessment, treatment, monitoring and review)
2. **Visit** each major stakeholder (senior staff, administrative department heads, etc.,) and discuss/evaluate:
    - The types (classifications) of information their department handles
    - How they handle paper documents with various types of information (Read more about data classification in the Asset Management Chapter.)
    - Use of encryption to protect sensitive or confidential information (Read more about encryption in the Cryptography Chapter.)
    - Third party service providers that they use to handle information on their behalf
    - External websites/portals where they enter and/or store information (Read more about third party service providers in the Supplier Relationships Chapter.)
    - Where they store institutional data (on their workstations, on the network, and/or external storage facilities like Dropbox or One Drive)
    - The potential impact of a loss of data integrity or availability and business continuity considerations (Read more about business continuity in the Information Security Aspects of Business Continuity Chapter.)
    - The specific compliance requirements that apply to this stakeholder's area such as HIPAA or PCI and whether these requirements are being addressed in a compliant manner. This can facilitate additional helpful conversations with legal affairs and auditors on campus. (Read more about compliance requirements in the Compliance Chapter.)

3. **Develop** a ranking system to help you sort and prioritize their responses

Evaluate risks and vulnerabilities associated with 'technology and people':

1. **Identify** IT-managed equipment/assets (use vulnerability scanning tools to conduct discovery scans and/or pull the information from an asset register)
2. **Run** vulnerability scans on those assets (servers, network equipment, PCI network devices, for example)
3. **Verify** where confidential information resides (use a Data Loss Prevention (DLP) tool to scan IT-managed workstations and network directories or try to identify this in general at stakeholder meetings) (See the HEISC Confidential Data Handling Blueprint for additional suggestions.)
4. **Have** staff and faculty completed security awareness training that emphasizes data protection? (See the Cybersecurity Awareness Resource Library for Suggestions.)

Expand the information security risk management program:

1. **Adopt** specific methodologies described in the standards and guidelines listed in #1 above
2. **Complete** a formal information security risk assessment across the university
3. **Take** a phased or incremental approach if the institution is large or has decentralized IT operations
4. **Outsource** risk assessments to third party service providers if you don't have resources to perform them
5. **Reevaluate** risks and vulnerabilities on a recurring basis as each risk assessment is a 'snapshot' at a point in time
6. **Explore** the use of GRC solutions that can assist with developing a formal risk management system.
7. **See** the HEISC GRC FAQ for an overview of GRC solutions.
8. **Review** the following resources for additional recommendations:
    - Learning While Doing: Two Institutions' Practical IT Risk Management Experiences
    - Practical Approaches to Effective Risk Management

Risk Management is the foundation of every good information security program. There are many approaches that an institution can take to identify risks that impact people, business processes (information handling), and technology. Prioritize identified risks and implement information security policies, controls, and compliance initiatives to assist with making information security program improvements.

Top of page

Overview

Risk management is an activity directed towards assessment, mitigation, and monitoring of risks to an organization. **Information security risk management** is a major subset of the enterprise risk management process, which includes both the assessment of information security risks to the institution as well as the determination of appropriate management actions and established priorities for managing and implementing controls to protect against those risks.

The risk management process involves setting institutional priorities and making key decisions in regards to what is sometimes called the institution's "appetite for risk". Primary direction in making decisions about risk acceptance needs to come from institutional leadership. Information security organizations may manage the risk management program but it's necessary to consult with institutional leadership about handling risks that cannot effectively be reduced or mitigated. The Risk Management Framework provides useful guidance to assist with developing these processes.

This process can be broadly divided into two components:

- Risk assessment
- Risk treatment

Risk assessment identifies, quantifies, and prioritizes risks against both criteria for risk acceptance and objectives relevant to the organization. The assessment results guide the determination of appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks. The assessment should include both a systematic approach to estimating the magnitude of risks and a process for comparing estimated risks against risk criteria to determine the significance of the risks.

The scope of a risk assessment can be either the whole organization, parts of the organization, an individual information system, or even specific system components or services. Performing a risk assessment in areas that include technology infrastructure also includes performing vulnerability assessments to help quantify risks. This process of assessing risks and vulnerabilities will need to be performed at recurring intervals, especially if an incremental approach is selected, to ensure that comprehensive and effective results are obtained. This will also ensure that constantly evolving changes in security requirements and/or significant changes are assessed. For example, IT will be implementing new products or services each year and new or additional risks may be introduced due to vulnerabilities that can be exploited.

Once a risk assessment is completed, **risk treatment** is the next step in the process. For each of the risks identified during a risk assessment, a risk treatment decision needs to be made. Possible options for risk treatment include:

- Knowingly and objectively accepting risks, providing they clearly satisfy the organization's policy and criteria for risk acceptance;
- Applying appropriate controls to reduce the risks;
- Avoiding risks by not allowing actions that would cause the risks to occur;
- Transferring the associated risks to other parties, e.g. insurers or suppliers.

For each of the risks where the treatment decision is to apply some level of risk mitigation, appropriate controls may be selected from other sections of the Guide or elsewhere (SANS Top Twenty Critical Security Controls, for example). Controls should be selected to ensure that risks are reduced to an acceptable level. Take into account applicable federal, state, and local statutes as well as other binding regulations. Additionally, consider institutional goals and objectives, operational requirements and constraints, the cost of implementing effective controls relative to potential harm of not implementing them, and the costs likely to result from one or more security failures.

It should be kept in mind that even after mitigating all current risks, achieving a 'state of complete security' is unlikely. Making continuous improvements through ongoing risk management activities will make a very positive impact.

A ***vulnerability assessment*** is basically an inventory of all vulnerabilities that is often thought of as a technical examination (e.g., network scanning). However, a complete vulnerability assessment would include the network, mission critical systems, physical environments, and processes.

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*) - in order to prioritize the potential mitigations that might be applied.

Risk management encompasses risk assessment and vulnerability assessment along with the mitigation. It also includes measuring the outcome of the process, and repeating the process again and again.

Top of page

Risk Assessment

Objective: Identify, analyze, prioritize, and treat information security risks.

Before discussing the different approaches to assess risk, it is necessary to define risk. NIST SP 800-30 *Risk Management Guide for Information Technology Practitioners* defines risk as a ***function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization***.

So the main components of a risk assessment are:

- Threats
- Vulnerabilities
- Impact (i.e., potential loss)
- Likelihood of occurrence (i.e., the probability that an event - threat successful exploit of a vulnerability - will occur)

There are a variety of risk assessment tools and methodologies that can be used, but all are basically divided into **quantitative** and **qualitative** risk assessments.

Quantitative Risk Assessment

Quantitative risk assessments attempt to assign a **monetary value** to the assets being assessed, a **monetary cost** to the impact of an adverse event, and **percentages** to the frequency of threats and the likelihood of events.

The monetary values and costs mentioned above are used to determine three elements needed to complete a quantitative risk assessment:

1) Single Loss Expectancy (SLE): What is the expected loss from a single event? Consider physical destruction or theft of assets, loss of data, stopped or delayed processing, and interruption of business processes.

> SLE = Asset Value x Impact (percent of asset loss incurred after an event)
>
> Example: A student registration system is worth $500,000 to an institution during registration period. A denial of service attack can keep the system offline for a third of that time
>
> SLE = $450,000 * 33% = $150,000
>
> When considering Impact include all associated costs:
>
> - Cost of repair or to replace equipment.
> - Value of the damaged equipment or lost data.
> - Cost to reload the data and to bring systems back online.
> - Lost staff productivity and potential income.

2) Annualized Rate of Occurrence (ARO): How many times is an event expected to happen in a year?

> Example: If the institution has three registration periods and a denial of service can happen in one of the three times then ARO = 33%. If it happens once every three years then ARO = 11%

3) Annual Loss Expectancy (ALO): What is the potential loss per year? Sometimes this value is referred to as the **magnitude of the risk**.

> ALO = SLE * ARO
>
> Example: It has been determined that the institution's registration system can be hit with a denial of service attack at one of the registration periods of the year.
>
> ALO = $150,000 * 33% = $50,000
>
> The ALO is taken in consideration when determining what controls to implement to mitigate the risk. Controls are implemented if their total cost is equal or less than the ALO.

Pros of Quantitative Risk Assessments

- Allows for a definition and communication of consequences of event occurrence in monetary terms
- Facilitates costs and benefits analysis during selection of mitigating controls.

Cons of Quantitative Risk Assessments

- It is very difficult, sometimes impossible, to assign a dollar value to assets being assessed and to the impact to those assets by all types of threats.
- Requires substantial time and staff resources.
- Values and costs are only as good and meaningful as the scope and accuracy of the amounts used to calculate them.
- Results of the assessment may be not precise and may be confusing.

Qualitative Risk Assessment

Qualitative risk assessments are scenario driven and do not attempt to assign a monetary value to the assets being assessed, or to the impact of an adverse event. They aim to rank the impacts of threats and criticality of assets into categories such as low, medium, and high. This ranking is for the most part subjective:

- Low—Minor inconvenience that could be tolerated for a short period of time.
- Medium—Can result in damage to the organization's assets which will require a moderate amount of time, effort, and money to repair.
- High—Can result in loss of organization reputation and goodwill. Can also result in a legal action or fine, and/or require a substantial amount of time, effort, and money to repair.

Pros of Qualitative Risk Assessments

- Allows for ordering risks according to priority.
- Does not require substantial time and staff resources.
- Can identify areas of greater risk in a short time and without significant expense.

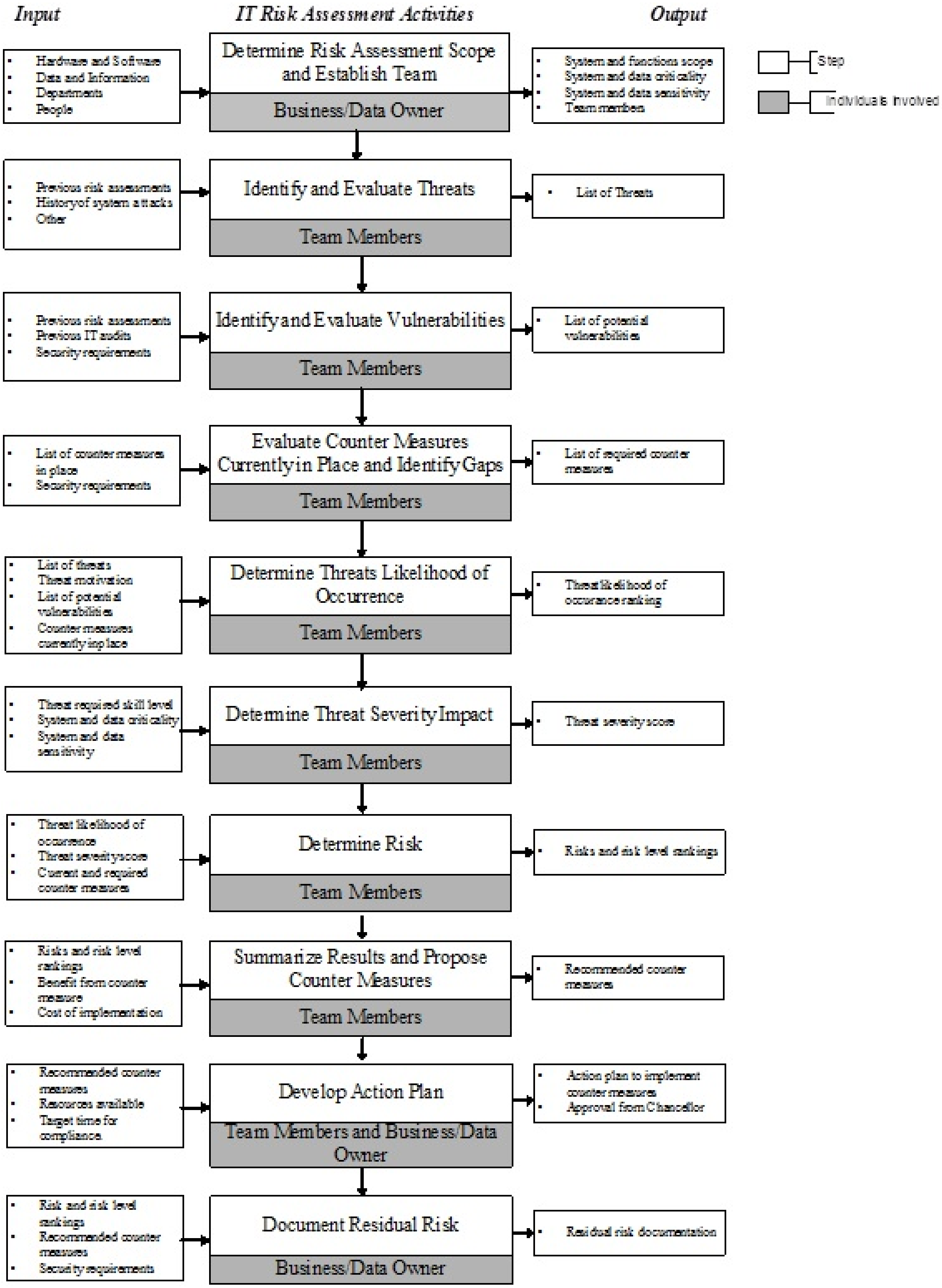
Cons of Qualitative Risk Assessments

- Results are approximations and subjective.
- Does not allow for probabilities and results using numerical / monetary measures.
- Cost-benefit analysis during selection of mitigating controls is subjective.

Sample Qualitative Risk Management Process from ISO/IEC 27005:2008

blocked URL

Sample Qualitative Risk Assessment Flow Adapted from NIST SP 800-30


Input
IT Risk Assessment Activities
Output
Step
Individuals involved
Hardware and Software
Data and Information
Departments
People
Determine Risk Assessment Scope and Establish Team
Business/Data Owner
System and functions scope
System and data criticality
System and data sensitivity
Team members
Previous risk assessments
History of system attacks
Other
Identify and Evaluate Threats
Team Members
List of Threats
Previous risk assessments
Previous IT audits
Security requirements
Identify and Evaluate Vulnerabilities
Team Members
List of potential vulnerabilities
List of counter measures in place
Security requirements
Evaluate Counter Measures Currently in Place and Identify Gaps
Team Members
List of required counter measures
List of threats
Threat motivation
List of potential vulnerabilities
Counter measures currently in place
Determine Threats Likelihood of Occurrence
Team Members
Threat likelihood of occurance ranking
Threat required skill level
System and data criticality
System and data sensitivity
Determine Threat Severity Impact
Team Members
Threat severity score
Threat likelihood of occurrence
Threat severity score
Current and required counter measures
Determine Risk
Team Members
Risks and risk level rankings
Risks and risk level rankings
Benefit from counter measure
Cost of implementation
Summarize Results and Propose Counter Measures
Team Members
Recommended counter measures
Recommended counter measures
Resources available
Target time for compliance
Develop Action Plan
Team Members and Business/Data Owner
Action plan to implement counter measures
Approval from Chancellor
Risk and risk level rankings
Recommended counter measures
Security requirements
Document Residual Risk
Business/Data Owner
Residual risk documentation

Adapted from NIST Special Publication 800-30 Risk Management Guide for Information Technology System, October 2001.

Top of page

ⓘ **Below are steps to follow in planning and conducting a qualitative risk assessment, aligned with the processes described above:**

Step 1: Determine Risk Assessment Scope and Establish Team

Some institutional, state, or federal laws and regulations specify the scope of a required risk assessment (e.g., HIPAA defines the scope as the assessment of the potential risks and vulnerabilities of electronic PHI that is electronically transmitted and stored by the covered entity.)

Others limit the scope of the risk assessment based upon the level of risk affecting IT and information assets (e.g., risk assessments conducted annually for high risk items and bi-annually for medium or low risk items.) The scope of a risk assessment will also include an analysis of how information is accessed, processed, and/or transmitted in business processes.

Before starting the risk assessment, develop a brief description of each technology or information asset's purpose, functionality, location, data and information criticality and sensitivity. Identify individuals using asset(s) and authentication procedures to gain access to the asset(s).

Determine what changes were made to the asset since the last risk assessment and identify from the documentation its technical components such as software, hardware, databases, and network technology.

The risk assessment team should include individuals from business units/data owners with expertise in business operations and processes as well as information security and information technology staff.

Step 2: Identify and Evaluate Threats

A threat is something or someone that can intentionally or accidentally exploit a specific vulnerability. Generally, there are three general types of threats:

- Natural – floods, earthquakes, tornadoes, etc.
- Human
  - Malicious – deliberate actions such as network attacks, unauthorized access, malware upload, etc.
  - Non Malicious – unintentional acts such as data entry errors, accidental deletions, etc.
- Environmental – power failure, water damage, heat, etc.

Step 3: Identify and Evaluate Vulnerabilities

A vulnerability is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised – accidentally triggered or intentionally exploited – and result in a security breach or a violation of the system's security policy. Generally, vulnerabilities can be divided as they relate to:

- Staff / Outsiders
- Facilities and equipment
- Applications
- Communications
- Software and operating systems

Step 4: Evaluate Controls Currently in Place and Identify Gaps

Controls are information security countermeasures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. Measures considered should combine technical, operational, and management controls to ensure adequate security.

Most institutions have already implemented numerous countermeasures to address security threats.   Considering the threats and vulnerabilities identified, evaluate if countermeasures currently implemented mitigate or eliminate the likelihood of occurrence of a threat's exercising a vulnerability.

When unacceptable gaps are found because there is a difference between the asset's minimum security requirements and the countermeasures in place, there are two possible courses of action. If there are additional controls that are feasible and can be implemented in a reasonable time, then recommendations for addressing those gaps are developed. Otherwise, the management must consider accepting or transferring the risk exposure.

Step 5: Determine Threat Likelihood of Occurrence

The following categories describe the likelihood that a potential vulnerability could be exercised by a given threat:

Likelihood	Score	Description
Frequent	5	Possibility of repeated incidents
Probable	4	Possibility of isolated incidents
Occasional	3	Possibility of occurring sometime
Remote	2	Not likely to occur
Improbable	1	Practically impossible

Example: *Flood may be considered to have a Remote likelihood of occurring. Thus the Likelihood Score for Flood is 2.*

Step 6: Determine Threat Impact Severity

The adverse impact of a successful threat exercise of a vulnerability can be described in terms of loss or degradation of the confidentiality, integrity, and availability of data. The following describes each impact.

- **Loss of Confidentiality:** Unauthorized, unanticipated, or unintentional disclosure of confidential data. Such disclosure could result in loss of public confidence, embarrassment, or legal action against System Administration.
- **Loss of Integrity:** Unauthorized, unanticipated, or unintentional destruction or changes made to data or IT system by either malicious or non-malicious acts. If loss of integrity is not corrected, continued used of corrupted data could result in inaccuracy, fraud, or erroneous decisions.
- **Loss of Availability:** Data is unavailable to its users impeding the performance of their functions.

The following categories describe the adverse impact of a successful threat exercise of a vulnerability and/or the level of skill required to successfully exploit it:

Severity	Score	Description
High	4	Elevated potential for loss; requires only some skill to exploit
Moderate	3	Moderate potential for loss; intermediate skills required to exploit
Low	2	Some potential for loss; requires a high level of skill to exploit
Insignificant or N/A	1	No real potential for loss; requires a very high level of skill to exploit

The Severity Score of each threat is the Average of the Impact Severity scores to the loss of confidentiality, integrity, and availability.

Example:

Type of Threat	Impact Severity to			Severity Score
	Confidentiality	Integrity	Availability	
Natural				
Flood	1	2	4	2.33

Step 7: Determine Risk

To quantify the risk, the numeric values added to each threat are rated based on the following factors:

- Severity of the threat.
- Likelihood of the threat.

Severity Level	Likelihood of Occurrence				
	Frequent	Probable	Occasional	Remote	Improbable
High	🟥	🟥	🟥	🟨	🟩
Moderate	🟥	🟥	🟨	🟨	🟩
Low	🟥	🟨	🟨	🟩	🟩
Insignificant	🟩	🟩	⬜	⬜	⬜

🟥	Undesirable risk and counter measures should be implemented or improved as soon as possible
🟨	Undesirable risk and counter measures should be implemented or improved in a reasonable amount of time
🟩	Acceptable risk and existing counter measures are likely adequate. Management review required.
⬜	Acceptable risk and existing counter measures are adequate. Management review not required.

Example: *The threat of Flood has a Likelihood of Occurrence of Remote (score of 2) and a Severity Level of Some (score of 2.33). The intersection of both values indicates that that Flood is an acceptable risk and the existing counter measures are likely adequate.*

Step 8: Summarize Results and Propose Additional Controls (Risk Treatment Process)

Considering countermeasures currently in place, propose a list of additional controls that could mitigate or eliminate the identified risks as required by security requirements. The goal is to reduce the level of risk to the IT asset to an acceptable level. Consider the following when proposing additional controls:

- Legislation and regulation requirements
- Impact on institutional technology infrastructure and operations
- Benefit derived from implementation
- Total cost of implementation

A cost-benefit analysis may be required to determine which controls are required and appropriate and to ensure that the costs of implementing the controls are justified by the corresponding level of risk reduction.

Step 9: Develop Action Plan

The action plan lists the controls selected to reduce risks and vulnerabilities to a reasonable and appropriate level. A cost-benefit analysis may be required as the basis for the selection of these additional controls.

The action plan prioritizes the implementation actions and projects the start and target completion dates. The action plan summary contains, at least, the following information:

- Selected controls (determined on the basis of feasibility, effectiveness, benefit to the institution, and cost)
- Prioritization
- Required resources for implementing the selected controls
- Responsible Party
- Start date for implementation
- Target completion date for implementation
- Operations and Maintenance requirements.

Step 10: Determine Residual Risk

The reduced level of institutional risk achieved by selecting and implementing additional controls is defined by an associated reduction in the number of flaws or errors, threat likelihood, or magnitude of impact.

Residual risk is the risk remaining after the implementation of the selected controls.

In practice, no information technology system or business process involving information handling is risk-free, and even with additional controls, it may not be possible to completely mitigate levels of risk. This is a normal condition.

As stated at the beginning of this document, the intent of this process is to implement security measures sufficient to reduce risks and vulnerabilities to an a cceptable level. If the residual risk affects only the business/data owner department, then the business/data owner department manager is responsible for deciding if the residual risk level is acceptable. If the residual risk affects multiple institutional departments or the institution’s network infrastructure, then the responsibility for accepting the residual risk is shared among executive officers (e.g., department head, CISO or CIO).

Documentation of residual risk contains, at least, the following information:

- A list of controls not considered reasonable or selected for implementation because of adverse impact on institutional technology infrastructure and operations, limited benefit derived from implementation, or cost of implementation.
- For each threat type:
    - Vulnerability description
    - Residual risk severity level
    - Impact severity level

Finally see Taking Risk Assessment from Project to Process: A Novel Approach, a presentation from the 2010 Security Professionals Conference that highlights an approach to risk assessment that is cost-effective, standardized, and simple to deploy.

Additionally, Verizon publishes an annual Data Breach Investigations Report (DBIR), which can be useful for focusing on known threat vectors. Also, several institutions are taking a more proactive approach, partnering with key stakeholders to introduce risk assessments into the project life cycle as early as possible.

Top of page

Risk Treatment

Objective: Develop a plan that identifies the controls necessary to reduce, retain, avoid, or transfer identified risks.

There are several ways to develop an effective risk treatment plan. One way is to follow the Risk Management Framework Phase 3, Mitigation Planning, that begins with the following two steps:

Step 1: Develop options to mitigate risk.

Step 2: Confer with management to agree upon strategy.

Alternatively, create a risk registry, which is a tool that can assist with managing and tracking risks. Record identified risks, their severity, and the actionable steps to be taken for each. Share with risk stakeholders and institutional leadership. Finally, organizations that have a mature risk management program in place may want to explore purchasing a solution to automate the business processes associated with governance, risk, and compliance (GRC). Before investing in a GRC solution, you may want to review the GRC FAQ to assist with making this decision.

Specific Risk Treatment Examples

1. Cyber Insurance is one way to reduce risks. However, if interested in this coverage, ask about the terms and conditions and review them carefully for potential exclusions. Most Cyber Insurance policies will not pay benefits if the insurance company determines that information affected during a data breach incident was not encrypted at rest. Additionally, they will scrutinize the protection applied to IT infrastructure where the information was stored to assess levels of protection and can deny the claim if they consider it inadequate or not meeting their standards. This coverage can be very expensive and conducting extensive research is warranted. Also take a look at the EDUCAUSE Cyber Insurance resource page and this informative article from the Wall Street Journal.
2. Developing processes similar to The Standard for Personal Digital Identity Levels of Assurance can potentially assist with risk mitigation.

Top of page

Resources

EDUCAUSE Resources

- IT Risk Management: Try This Exercise at Your Institution, an example of using the EDUCAUSE Top Ten IT Issues as a guide to inform risk management practices (from Educause Review Online)
- Practical Approaches to Effective Risk Management, Presentation at EDUCAUSE Annual Conference, 2011
- Proactive Compliance through Information Systems Risk Management, Presentation at the MidAtlantic Regional Conference, 2011
- Cyber Insurance resource page for EDUCAUSE publications, presentations and other resources on this topic.
- Taking Risk Assessment from Project to Process: A Novel Approach Presentation at the Security Professionals Conference, 2010
- Risk Management Framework for an adaptable approach to risk management oriented toward higher education.
- Security Risk Management resource page for EDUCAUSE publications, presentations and other risk assessment and analysis resources.
- Risk Management resource page for EDUCAUSE publications, presentations and other resources on this topic.
- Information Security Program Self-Assessment Tool is intended to help a CIO or CISO evaluate and track the maturity of an information security program.
- Foundations for Effective Security Risk and Program Assessment, EDUCAUSE Security Professionals Conference 2010
- GRC FAQ: Frequently Asked Questions about Governance, Risk, and Compliance (GRC) Systems, 2012

Initiatives, Collaborations, & Other Resources

- Statement on Standards for Attestation Engagements (SSAE) No. 16 (formerly SAS 70) focuses on the design of controls and their operating effectiveness.
- Payment Card Industry Standard (PCI)
- Verizon's Annual Data Breach Investigations Report provides known threat vector information
- Evaluating Cloud Risk for the Enterprise: A Shared Assessments Guide
- The Forrester Wave: Governance, Risk, and Compliance Platforms
- Gartner's Magic Quadrant for IT Risk Management (includes a list of products to automate effective IT risk management processes)

Top of page

Standards

ISO	NIST	COBIT	PCI DSS	2014 Cybersecurity Framework	HIPAA Security

ISO 31000: 2009 **ISO/IEC 31010:2009** **ISO/IEC 27002:2013** **ISO/IEC 27005:2011**	**800-30**: Risk Management Guide for Information Technology Systems **800-53**: Recommended Security Controls for Federal Information Systems and Organizations	**APO12.01** **APO12.02** **APO12.03** **APO12.04** **APO12.05** **APO12.06** **APO13.02** **BAI02.03** **BAI04.02** **DSS04.02**	PCI DSS, v3.0, released November 2013, is a standard for assisting with compliance with the Payment Card Industry Data Security Standard (PCI DSS). The Self-Assessment Questionnaire is a validation tool intended to assist merchants and service providers in self-evaluating their compliance.	**ID.RA-1** **ID.RA-2** **ID.RA-3** **ID.RA-4** **ID.RA-5** **ID.RA-6** **ID.RM-1** **ID.RM-2** **ID.RM-3**	**45 CFR 164.308(a)** **45 CFR 164.316(a)** **45 CFR 164.316(b)** **45 CFR 164.306**

Top of page

Questions or comments? Contact us.