Risk Assessment Procedure

NIST – Risk Assessment

Aurora University

May 2022

AURORA UNIVERSITY

Procedure: Risk Assessment Procedure	
Issue Date:	Procedure Number:
Revision Number:	NIST Control: RA-1
Revision Date:	Owner: ISO

Contents

1. Overview

Reliance on technology by institutions increases the risk of vulnerability exploitation, with new threats occurring in the environment on a daily basis. Aurora University's ability to identify and remediate risk is critical to protecting its information assets.

Risk assessments inform decision makers and support risk responses by identifying:

a. Relevant threats to institutions or threats directed through institutions against other institutions;
b. Vulnerabilities, both internal and external to institutions;
c. Impact (i.e., harm) to the institution, based off potential of threats exploiting vulnerabilities; and
d. Likelihood that harm will occur.

The results of risk assessments provide senior leadership/executives with the information needed to determine appropriate courses of action in response to identified risks.

2. Scope

The scope of this procedure includes all information assets governed by Aurora University. All personnel and third parties who have access to or utilize assets of the Institution, including data at rest, in transit or in process shall be subject to this Procedure.

3. Definitions

Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. See Information System-Related Security Risk. [CNSSI No. 4009]

Risk Management: The process of identifying, estimating, and prioritizing risks to institutional operations (including mission, functions, image, reputation), institutional assets, individuals, other institutions, and the Nation, resulting from the operation of an information system. [NIST SP 800-39]

4. Roles and Responsibilities

Board of Directors: The Board of Directors is ultimately responsible for ensuring that the institution has an adequate and effective risk manage process and that this process is reviewed by Management at regular intervals. The Board is ultimately responsible for approving the risk management process, makes key strategic decisions addressing risk, and fulfills its governance responsibilities by providing necessary oversight of management.

Management: The Chief Information Officer (CIO) and designee will appoint responsibility to the heads of departments or institutional units for implementing the risk assessment procedure and ensure that the institution adheres to this procedure.

Employees (faculty, staff, and student workers): Understanding and implementing risk management on a daily basis is an important function for all faculty, staff and student workers. All faculty, staff and student workers are expected to be knowledgeable of institutional policy and procedural requirements, take other reasonable actions to not create unnecessary exposure and ensure that their supervisors are aware of risks as deemed appropriate.

5. Training

Aurora University Management will determine the nature and extent of faculty, staff and student worker training relating to risk management, subject to Board approval.

6. Risk Assessment

6.1 Introduction

Aurora University employs a qualitative risk assessment approach leveraging the NIST SP 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations*. The Risk Assessment is a multi-phased process that identifies and prioritizes security risks across the enterprise.

The Risk Assessment is to be conducted by a team of certified security assessors with technical and business knowledge of the institution’s information technology assets and business processes.

6.2 Risk Assessment Process

The Risk Assessment shall be a structured process consisting of the following phases:

Phase 1: Planning – Organization of the assessment process.

a) Scope Definition – Identification of assets, facilities, applications, services, locations and other boundaries.
b) Team Development – Identification of Subject Matter Experts (SMEs) for each security domain.
c) Schedule Development – Organizing of SME and assessor schedules for interview sessions.
d) Historical Analysis – Evaluation of past performance of past assessment and audits, known vulnerabilities, policy exceptions and other assumptions that may have influenced the results of the current assessment.

Phase 2: Security Assessment – Identification of vulnerabilities.

a) Subject Matter Expert Interviews – Discovery and evaluation of security controls across all in-scope people, processes, and technologies.
b) Artifact Analysis – Evaluation policies, procedures, documentation, reports, logs, and other artifacts.

Phase 3: Risk Management – Characterization of vulnerabilities followed by calculation and prioritization of risks.

Phase 4: Findings Documentation – Development of Findings documentation and reports.

Phase 5: Findings Presentation – Presentation of Findings (if applicable).

6.3 Risk Management Components

Risk Management procedures are designed to evaluate a given vulnerability, quantify the vulnerability's potential impact on the institution, and the likelihood that a threat agent will exploit the vulnerability. Together, these factors speak to the overall risk associated with an asset or system. Once the risk is understood, Risk Management mitigates the risk through the application of disciplines covering:

- Controlled transfer of the risk;
- Minimizing impact or changing the likelihood of occurrence; and
- Acceptance of the risk.

The following is the Information Security & Risk Management rating methodology adopted and approved by Aurora University:

- Risk = Likelihood x Impact

6.4 Risk Scoring

Likelihood/Impact Ranking	Likelihood/Impact Score	Definition
High	5	• Threat is very likely to occur • Critical Impact if threat is exploited
Medium – High	4	• Threat is somewhat likely to occur • High Impact if threat is exploited
Medium	3	• Threat is likely to occur • Moderate Impact if threat is exploited
Medium – Low	2	• Threat is unlikely to occur • Low Impact if threat is exploited
Low	1	• Threat is very unlikely to occur • Minimal Impact if threat is exploited

6.1.1. Step 1: Identifying Threats

The first step is to identify the threat/vulnerability pairs: the threat agent involved, the attack used, the vulnerability involved, and the impact of a successful exploit on the business. There may be multiple possible groups of attackers, or even multiple possible business impacts. In general, it's best to err on the side of caution by using the worst-case option, as that will result in the highest overall risk.

6.1.2. Step 2: Factors for Estimating Likelihood

Once the potential risk has been identified the next step is to determine how serious the risk is. To determine the seriousness of the risk - estimate the "likelihood" of its occurrence. At the highest level, this is a rough measure of how likely this particular vulnerability is to be uncovered and exploited by an attacker. We do not need to be over-precise in this estimate. The *Risk Scoring* table is used to assign ratings for likelihood.

There are a number of factors that can help us figure this out. The first set of factors is related to the threat agent involved. The goal is to estimate the likelihood of a successful attack from a group of possible attackers.

Note: There may be multiple threat agents that can exploit a particular vulnerability, so it's usually best to use the worst-case scenario. For example, an insider may be a much more likely attacker than an anonymous outsider - but it depends on a number of factors. Each factor has a set of options, and each option has a likelihood rating from 1 to 5 associated with it. These ratings are utilized in the risk calculator tool to quantify the overall likelihood.

6.1.1.1. Threat Agent Factors

The first set of factors is related to the threat agent involved. The goal here is to estimate the likelihood of a successful attack by this group of threat agents. Factors include:

1. Skill level

   What level of skill is required on the part of the threat agent in order to exploit the vulnerability?

   a) Security penetration skills
   b) Network and programming skills
   c) Advanced computer user
   d) Some technical skills
   e) No technical skills

2. Motive

   How motivated is this group of threat agents to find and exploit this vulnerability?

   a) Low or no reward
   b) Possible reward
   c) High reward

3. Opportunity

   What resources and opportunity are required for this group of threat agents to find and exploit this vulnerability?

   a) Full access or expensive resources required
   b) Special access or resources required
   c) Some access or resources required

d) No access or resources required

4. Size

   What is the size of the population to which the vulnerability is visible?

   a) Developers
   b) System administrators
   c) Intranet users
   d) Partners
   e) Authenticated users
   f) Anonymous Internet users

6.1.1.2. Vulnerability Factors

The next set of factors is related to the vulnerability involved. The goal here is to estimate the likelihood of the particular vulnerability being discovered and exploited. Assume the threat agent selected above.

1. Ease of Discovery

   How easy is it for this group of threat agents to discover this vulnerability?

   a) Practically impossible
   b) Difficult
   c) Easy
   d) Automated tools available

2. Ease of exploit

   How easy is it for this group of threat agents to actually exploit this vulnerability?

   a) Theoretical
   b) Difficult
   c) Easy
   d) Automated tools available

3. Awareness

   How well known is this vulnerability to this group of threat agents?

   a) Unknown
   b) Hidden
   c) Obvious
   d) Public knowledge

4. Intrusion Detection

How likely is an exploit to be detected?

a) Active detection in application
b) Logged and reviewed
c) Logged without review
d) Not logged

6.1.3. Step 3: Factors for Estimating Impact

When considering the impact of a successful attack, it's important to realize that there are two kinds of impacts. The first is the "technical impact" on the application, the data it uses, and the functions it provides. The other is the "business impact" on the institution operating the application.

Ultimately, the business impact is more important. However, you may not have access to all the information required to figure out the business consequences of a successful exploit. In this case, providing as much detail about the technical risk will enable the appropriate business representative to make a decision about the business risk.

Again, each factor has a set of options, and each option has an impact rating from 0 to 9 associated with it. These ratings are utilized in the risk calculator tool to quantify the overall impact.

6.1.1.3. Technical Impact Factors

Technical impact can be broken down into factors aligned with the traditional security areas of concern: confidentiality, integrity, availability, and accountability. The goal is to estimate the magnitude of the impact on the system if the vulnerability were to be exploited.

1. Loss of confidentiality

   How much data could be disclosed and how sensitive is it?

   a) Minimal non-sensitive data disclosed
   b) Minimal critical data disclosed
   c) Extensive non-sensitive data disclosed
   d) Extensive critical data disclosed
   e) All data disclosed

2. Loss of integrity

   How much data could be corrupted and how damaged is it?

a) Minimal slightly corrupt data
b) Minimal seriously corrupt data
c) Extensive slightly corrupt data
d) Extensive seriously corrupt data
e) All data totally corrupt

3. Loss of availability

   How much service could be lost and how vital is it?

   a) Minimal secondary services interrupted
   b) Minimal primary services interrupted
   c) Extensive secondary services interrupted
   d) Extensive primary services interrupted
   e) All services completely lost

4. Loss of accountability

   Are the threat agents' actions traceable to an individual?

   a) Fully traceable
   b) Possibly traceable
   c) Completely anonymous

6.1.1.4. Business Impact Factors

The business impact stems from the technical impact but requires a deep understanding of what is important to the institution running the application. In general, you should be aiming to support your risks with business impact, particularly if your audience is executive level. The business risk is what justifies investment in fixing security problems.

An asset classification guide and/or a business impact reference guide is used to help formalize what is important to the institution. These standards can help you focus on what's truly important for security. In lieu of the guides utilize an interview technique with key institution process owners to ascertain critical institution functions and associated technologies.

The factors below are common areas:

1. Financial damage

   How much financial damage will result from an exploit?

a) Less than the cost to fix the vulnerability
b) Minor effect on annual profit
c) Significant effect on annual profit
d) Bankruptcy

2. Reputation damage

Would an exploit result in reputation damage that would harm the institution?

a) Minimal damage
b) Loss of major accounts
c) Loss of goodwill
d) Brand damage

3. Non-compliance

How much exposure does non-compliance introduce?

a) Minor violation
b) Clear violation
c) High profile violation

4. Privacy violation

How much personally identifiable information could be disclosed?

a) One individual
b) Hundreds of people
c) Thousands of people
d) Millions of people

6.1.4. Step 4: Determining the Severity of the Risk

This step involves putting together the likelihood estimate and the impact estimate to calculate an overall severity for this risk. Determine whether the likelihood is LOW, MEDIUM-LOW, MEDIUM, MEDIUM-HIGH or HIGH. Repeat the process for the impact. The result is a final risk rating for each vulnerability.

6.1.5. Step 5: Prioritize Risks and Plan Remediation

With each required vulnerability risk score calculated, high risk item evaluation can be prioritized above lower risk items. Planned remediation efforts should be completed in accordance with the previous listed options including:

- Controlled transfer of the risk
- Minimizing impact or changing the likelihood of occurrence
- Acceptance of the risk

7. Risk Assessment Schedule

Risk assessments will be conducted in accordance with the following schedule:

Name	Type	Description	Frequency	Department Responsible
Organizational Risk Assessment	NIST 800-171 Assessment	Identification, evaluation, and prioritization of institutional risks to include people, process, and technology.	Annually	Information Technology
External Vulnerability Scans	Vulnerability Assessment	External scan of publicly accessible IP address space	Bi-Annually	Information Technology Services
Internal Vulnerability Scans	Vulnerability Assessment	Authenticated scan of internal network resources	Bi-Annually	Information Technology Services
Application Security Assessment	Penetration Test	Assessment of application security design practices and technical vulnerabilities	Annually	Information Technology Services
			Every 2 Years	

Network Security Design Assessment	Vulnerability Assessment	Penetration test of entire network.		Information Technology Services
Wireless Security Assessment	Vulnerability Assessment	Security review of wireless access point configuration and availability	Annually	Information Technology Services
Physical Security Assessment	Penetration Test	Physical test of all facilities critical to the institution	Annually	Information Technology Services

8. Enforcement

Any personnel found to have violated this procedure may be subject to disciplinary action up to and including termination of employment.

9. References

- CNSSI No. 4009 – *National Information Assurance (IA) Glossary*
- NIST SP 800-39 - *Managing Information Security Risk*
- NIST SP 800-30 - *Guide for Conducting Risk Assessments*
- OWASP Risk Rating Methodology

10. Revision History

Version	Date	Author	Revisions
1.0	3-02-2022	GreyCastle Security	Initial Draft

1.1	5-26-2022	Aurora University Team	Approval/Effective