Vulnerabilities and the Risk Management Process

Reading

1h

Status | Incomplete

Introduction

The Risk Management Process is a set of steps and procedures undertaken by an organization to document their assets, measure security and privacy controls they use, and gauge the effectiveness of those controls. Vulnerability assessments are a small but important component of the overall Risk Management Process of an organization.

The goal of this process is to enlighten those responsible for protecting the organization and its assets, and to support them in making decisions about controlling the risk of information security threats to the organization. In other words, working to reduce the chance that a threat or bad actor could be successful at doing damage to a business and its assets.

Vulnerability Assessment Within the Risk Management Process

You are likely familiar with NIST's Risk Management Framework. To refresh your memory, here is a diagram of the seven stages of the process:

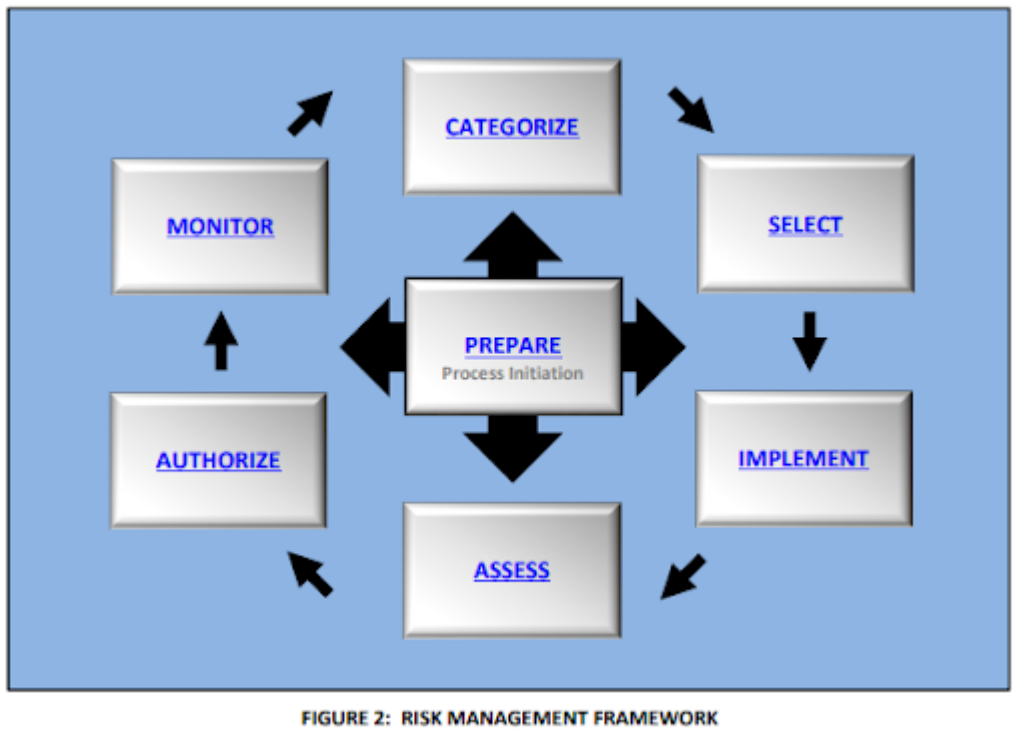

FIGURE 2: RISK MANAGEMENT FRAMEWORK

(Image source: NIST Risk Management Framework, Chapter 2, pg 9)

Which stage of the framework do you think is relevant to vulnerability assessments?

Think about your answer, then click “Toggle Answer” to find out.

If you chose “Assess”, you’re correct.

This stage comes after the planning and implementation portions of the process and is specifically aimed at measuring if the security and privacy controls in place are actually effective or not, and whether there are additional vulnerabilities that need to be dealt with.

Toggle Answer

Understanding Security and Privacy Controls

Before you dive into vulnerability assessments, you’ll want to be certain that you’ve considered the full breadth of what constitutes “security and privacy controls”. The term refers to all the various approaches an organization puts in place to protect the security of its assets and the privacy of its information. Security and privacy controls cover three areas of the organization, sometimes referred to as the three pillars of Cyber Security:

- People
- Processes
- Technology

People

These are the employees, users, stakeholders, or anyone that is involved with the organization who could potentially impact the security of the organization, positively or negatively.

Processes

This refers to how things are done in the organization. Company policies and procedures, and the resultant workflows and methods, ensure things are being done in a way that will help the company to be productive and successful. Included in this is the protection of the assets and people of the organization.

Technology

This refers to all the various tools, software, methodologies, approaches, etc. used by the company to ensure that business is successful and secure.

Vulnerability Assessment as an Approach

There are a number of approaches you can take to assess the work done to secure your organization:

- Test the controls directly (i.e., penetration testing).
- Evaluate the setup, configurations, documentation, and surrounding setup and security (like physical security).
- Interview stakeholder parties that are involved with the target or asset in question to gain perspective on what they see and experience and the procedures that are in place.

Performing a vulnerability assessment falls within the first approach, as you are testing the implemented security and privacy controls directly.

Purpose of Vulnerability Assessments

Like the Risk Management Process itself, vulnerability assessments and scans are not a 'one-and-done' activity. They are run, evaluated, and reported on repeatedly as part of an ongoing and regular evaluation of the organization's security posture. They should be considered part of the ongoing monitoring that is done to ensure the organization and its assets stay safe.

The overall benefits of performing regular vulnerability assessments can include:

- Identification of gaps in an organization's Risk Management Process
- Identification of vulnerabilities in the implemented security and privacy controls
- Confirmation of the effectiveness of previously implemented mitigations
- Prioritization of vulnerability mitigation plans
- Support for monitoring and security situational awareness within the organization
- Contribution to decisions regarding system authorizations
- Input for budgetary and capital investment decisions

(summarized from: Assessing Security and Privacy Controls in Information Systems and Organizations, chapter 1, pgs 1 and 3)

Vulnerability Assessments and Organizational Goals

A vulnerability assessment is not just about looking for holes in the organization's security posture that bad actors might be able to exploit, it is about the overall picture and support of the organization and its business process and goals.

From this wider scope of business management, the Risk Management Process is driven by the goals of the organization, and decisions related to the health and viability of that organization. Documenting and measuring the threats to the organization helps company executives meet very specific goals:

- Know what assets the organization has and make decisions regarding the sensitivity and criticality of each individual asset (these decisions will affect how each asset is used and protected).
- Understand what threats exist for each asset and what risks those threats may pose to the organization itself (the severity of each potential risk and how badly it could affect the business if it happens).
- Decide how much risk the business can safely handle.
- Make informed decisions about how to deal with each potential risk to the organization (accept, avoid, mitigate, or transfer).

> If you are in the early stages of your Cyber Security career, it's unlikely that you will be making decisions on the approach, scope, and focus of a vulnerability assessment.
>
> These decisions usually take place at the higher levels of an organization. However, they usually consider advice from the organization's security team, which is where you might make recommendations.

Policies and Procedures

Drawing on the information from vulnerability assessment reports and other parts of the Risk Management Process, company executives will formalize business-wide decisions by developing policies and procedures that will impact all levels of the business.

Take ongoing monitoring of networks, devices, and vulnerabilities as an example. Monitoring does not live only in the domain of the security team. It is important to all levels of the organization, and requires involvement and support from different departments. Policies and procedures that include ongoing monitoring practices (including regular vulnerability assessments) ensure that things are done in a responsible and consistent manner. They will outline what should be monitored and tested, how frequently, who should be involved, who should be notified, and what kinds of information should be communicated, as well as how and when.

Further Reading

Deep dive into how monitoring should be handled within an organization and how it is integrated throughout all levels of the organization.

> As you read, consider how and where vulnerability assessments come into play, and what parts of a monitoring policy would be informed by the results and recommendations in a vulnerability assessment report.

NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

Key Takeaways

In this reading you should have:

- Become more aware of how vulnerability assessments are a targeted monitoring activity that checks on the up-to-date effectiveness of an organization's security and privacy controls implemented
- Understood how vulnerability assessments can contribute to improving not only the security posture of the business, but also its Risk Management Process, and that they require buy-in and contributions from all levels of the organization
- Connected the importance of company policies and procedures to the planning and completion of any and all monitoring processes

Conclusion

Nothing that is done by the security team of an organization is standalone or on a whim. In fact, not only is the whole organization affected by the activities of the security team, they also contribute to and are part of the company's security efforts and posture. Everyone plays a vital role.

✓ Mark Completed

Previous
Vulnerability Assessments Knowledge Check

Next
Vulnerability Management Best Practices

How well did this activity help you to understand the content?

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W05D4

Thu Jul 25

- Lectures (1)
- Work (8)

6 hrs

- Case Study: Vulnerability Assessment Scan
- Discussion: Vulnerability Assessment Scan Case Study
- Vulnerability Assessments Knowledge Check
- Vulnerabilities and the Risk Management Process
- Vulnerability Management Best Practices
- Vulnerability Management Process Knowledge Check
- Vulnerability Assessment Report Templates
- Report Templates Review

W05D4 Schedule »