Risk Assessment Guide Adapted from NIST SP 800-30 Rev. 1

v1.0.1

Author:

Eldon Gabriel

July 11, 2025

TABLE OF CONTENTS

Disclaimer: This document is adapted from NIST SP 800-30 Rev. 1. The original publication is publicly available from the National Institute of Standards and Technology (NIST).

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.0.0	02/21/2025	Eldon G.	Initial draft.
v1.0.1	07/11/2025	Eldon G.	Added a Conclusion section with Key Takeaways.

Disclaimer: This document is adapted from NIST SP 800-30 Rev. 1. The original publication is publicly available from the National Institute of Standards and Technology (NIST).

SECTION 1.0: RISK ASSESSMENT GUIDE

Adapted from NIST SP 800-30 Rev. 1

1.1 Introduction

NIST SP 800-30 provides a structured approach to assessing risk in information systems. This guide outlines strategies for identifying, analyzing, and mitigating risks, helping organizations allocate resources effectively and prioritize remediation efforts.

Note: *NIST's Computer Security Resources Center contains more information on SP 800-30 Rev. 1.*

1.2 Threat Sources

Threat sources are entities or circumstances that can negatively impact an organization's information systems. These sources can be internal or external and may have different capabilities and intentions.

Type	Examples	Description
Standard User	Employee, Customer	Accidental or intentional exploitation of system vulnerabilities.
Privileged User	System Administrator	Elevated access rights can lead to misuse or compromise.
Group	Competitor, Supplier, Business Partner, Nation-State	Organized efforts to exploit vulnerabilities.
Outsider	Hacker, Hacktivist, Advanced Persistent Threat (APT)	Malicious actors are targeting organizational assets.
Hardware	Storage, Processing, Communications	Failures due to resource depletion or aging infrastructure.
Software	Operating Systems, Networking, Malicious Software	Vulnerabilities that can be exploited for attacks.
Operational Environment	Temperature Controls, Humidity, Power Supply Failures	Environmental factors affecting system integrity.
Natural Hazards	Power Outages, Extreme Weather Events	External conditions are disrupting operations.

1.3 Threat Events

Threat events occur when a threat source exploits a vulnerability, causing damage or harm to an organization's information systems.

Example	Description
Reconnaissance & Surveillance	Threat actors gather intelligence on vulnerabilities.
Exfiltration of Sensitive Information	Malicious software extracts confidential data.
Data Alteration or Deletion	Critical business information is modified or erased.
Creation of Counterfeit Certificates	Unauthorized entities forge certificates to bypass security controls.
Persistent Network Sniffers	Malicious software intercepts and monitors network traffic.
Denial of Service (DoS) Attacks	Attackers flood systems with traffic, disrupting operations.
Disruption of Mission-Critical Operations	Business processes are rendered non-functional.
Obfuscation of Future Attacks	Threat actors bypass intrusion detection and logging mechanisms.
Man-in-the-Middle Attacks	Unauthorized interception and modification of communications.

1.4 Likelihood of a Threat Event

Likelihood measures the probability that a threat event will occur, based on available evidence, historical data, and expert judgment.

Likelihood Ratings

Qualitative Value	Quantitative Value	Description
High	3	The event is almost certain to cause a severe impact.
Moderate	2	The event is likely to affect operations.
Low	1	The event is unlikely to have minimal effects.

1.5 Severity of a Threat Event

Severity assesses the potential impact of a threat event on business operations.

Severity Ratings

Qualitative Value	Quantitative Value	Description
High	3	Severe or catastrophic effects on operations.
Moderate	2	Significant disruption but not total failure.
Low	1	Minor impact with negligible consequences.

SECTION 2.0: CONCLUSION

2.1 Key Takeaways

- A clear risk assessment approach helps find and rank threats to information systems.
- Knowing where threats come from and how they happen lets you focus on fixing the right problems.
- Evaluating likelihood and severity quantifies risk, helping allocate resources effectively.
- Doing regular risk assessments keeps the organization stronger against new cyber threats.
- Following NIST SP 800-30 principles helps meet standards and improves overall security.