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

v1.0.2

Author:

Eldon Gabriel

March 17, 2026

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 conclusion section outlining key takeaways.
v1.0.2	03/17/2026	Eldon G.	Updated document title and finalized formatting for portfolio publication

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).

1.0 RISK ASSESSMENT GUIDE

Adapted from NIST SP 800-30 Rev. 1

1.1 Introduction

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

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

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).

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	Exploiting vulnerabilities through organized efforts
Outsider	Hacker, Hacktivist, Advanced Persistent Threat (APT)	Malicious actors target organizational assets.
Hardware	Storage, Processing, Communications	Failures owing to resource depletion or aging infrastructure.
Software	Operating Systems, Networking, Malicious Software	Vulnerabilities that can be exploited in attacks.
Operational Environment	Temperature Controls, Humidity, Power Supply Failures	Environmental factors affecting system integrity
Natural Hazards	Power Outages, Extreme Weather Events	External conditions disrupt operations.

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).

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 regarding vulnerabilities.
Exfiltration of Sensitive Information	Malicious software extracts confidential data.
Data Alteration or Deletion	Critical business information is either 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 became 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.

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).

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 have a severe impact.
Moderate	2	This event is likely to affect operations.
Low	1	This 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	Slight impact with negligible consequences.

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).

2.0 CONCLUSION

2.1 Key Takeaways

- A clear risk assessment approach helps identify and rank threats to information systems.
- Understanding the sources and mechanisms by which threats occur enables focus on fixing the correct problems.
- Evaluating likelihood and severity quantifies risk and helps allocate resources effectively.
- Regular risk assessments strengthen an organization against new cyber threats.
- Adopting NIST SP 800-30 principles helps meet standards and improves overall security.

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).