

Introduction to Security Risk Assessment

Introduction to Security Risk Assessment

Key concepts, steps, and best practices for evaluating and managing security threats.

1. What Is a Security Risk Assessment?

Aspect	Description
Definition	A systematic process to identify, analyze, and prioritize potential threats to an organization's assets and to determine appropriate controls.
Goal	Reduce the likelihood and impact of security incidents while aligning protection measures with business objectives and regulatory requirements.
Scope	Can cover physical security, information/cyber security, personnel security, operational processes, and supply chain risks.

2. Core Terminology

Term	Meaning
Asset	Anything of value to the organization (data, hardware, facilities, reputation).
Threat	A potential cause of an unwanted incident (e.g., malware, insider theft, natural disaster).
Vulnerability	A weakness that can be exploited by a threat (e.g., unpatched software, weak passwords).
Risk	The combination of likelihood of a threat exploiting a vulnerability and the impact of that event.
Control / Safeguard	A measure (technical, administrative, or physical) that reduces risk.
Residual Risk	Risk remaining after controls are applied.
Acceptable Risk	The level of risk the organization decides it can tolerate.

3. Standard Risk Assessment Frameworks

Introduction to Security Risk Assessment

Framework	Typical Use	Key Features
NIST SP 800-30	U.S. federal & private sector	Detailed step-by-step process; integrates with NIST CSF.
ISO/IEC 27005	International organizations	Aligns with ISO/IEC 27001 ISMS; emphasizes continual improvement.
OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)	Large enterprises	Focuses on organizational culture and self-assessment.
FAIR (Factor Analysis of Information Risk)	Quantitative modeling	Uses probability and financial impact to produce monetary risk values.
CIS Controls	Small-to-medium businesses	Prioritized, actionable security controls linked to risk mitigation.

Choose a framework that matches your regulatory environment, industry, and maturity level.

4. The Risk Assessment Process (Six-Step Model)

1. Define Scope & Context

- Identify business units, processes, and assets to be assessed.
- Determine regulatory, contractual, and stakeholder requirements.

2. Asset Identification & Valuation

- Create an asset register (hardware, software, data, facilities).
- Assign value based on confidentiality, integrity, availability (CIA) and business impact.

3. Threat & Vulnerability Identification

- **Threat sources:** cyber attackers, insiders, natural events, suppliers.
- **Vulnerability sources:** outdated patches, misconfigurations, lack of training.
- Use threat intelligence feeds, vulnerability databases (CVE, NVD), and interviews.

4. Risk Analysis

- **Qualitative:** High/Medium/Low ratings based on expert judgment.

Introduction to Security Risk Assessment

- **Quantitative:** Likelihood × Impact (often expressed as a dollar figure).
- Tools: risk matrices, Monte Carlo simulations, FAIR calculators.

5. Risk Evaluation & Prioritization

- Compare analyzed risk against the organization's risk tolerance thresholds.
- Rank risks to focus resources on the most critical items.

6. Risk Treatment (Mitigation)