Preparing for Your First Risk Assessment

Name: Ammar Yasser Mohamed
Enterprise Security Department - Summer 2025

Date: August 3, 2025

What is a Risk Assessment?

A risk assessment is a structured process to identify, evaluate, and prioritize risks to an organization's assets, operations, and people. It allows decision-makers to implement appropriate controls and allocate resources effectively.

Goal: Identify potential threats, assess vulnerabilities, and determine the impact if the threat exploits a vulnerability.

Step-by-Step Risk Assessment Preparation

1. Define the Scope

Begin by clearly stating what systems, processes, or departments will be included.

Example: A risk assessment for a web application should cover:

- The application servers
- Database and storage
- APIs and third-party integrations
- Authentication and user roles

2. Understand Risk Terminology

- **Asset:** Something valuable (e.g., customer data, server).
- **Threat:** Something that can cause harm (e.g., malware).
- **Vulnerability:** Weakness that can be exploited (e.g., outdated software).
- **Risk:** Likelihood that a threat will exploit a vulnerability and cause impact.

Example:
Asset: HR Database
Threat: Insider leaking salary information
Vulnerability: No access logging or user monitoring
Risk: High reputational and legal impact

3. Choose a Risk Framework or Model

Frameworks guide your process and give structure.

- **NIST SP 800-30:** Widely used in federal and enterprise environments.
- **ISO/IEC 27005:** Part of the ISO 27001 family.
- **OCTAVE:** Organizational-centric risk analysis.
- **FAIR:** Quantitative approach for risk financial modeling.
- **STRIDE:** Used for threat modeling in software systems.

4. Build an Asset Inventory

Create a list of all assets in the scope.

Categories:

- Physical (servers, laptops)
- Logical (databases, software, APIs)
- People (admins, HR, developers)
- Processes (accounting, authentication)

Example Entry:

- **Name:** Payroll System
- **Owner:** HR Department
- **Type:** Web Application
- **Data Sensitivity:** High

5. Identify Threats and Vulnerabilities

Sources:

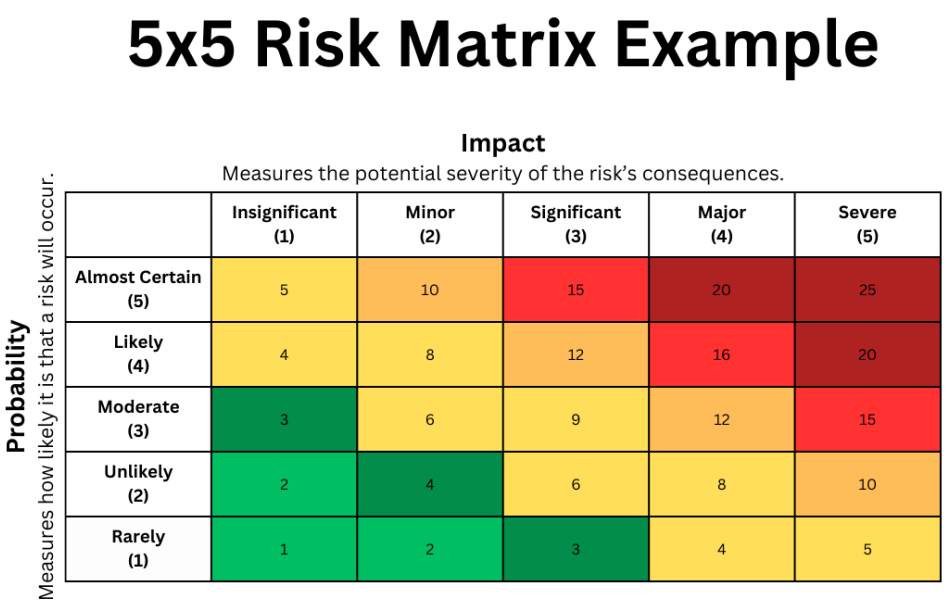
- Threat intelligence feeds
- MITRE ATT&CK
- OWASP Top 10
- Internal audits

Example:

- **Threat:** Ransomware
- **Vulnerability:** No EDR software on endpoints
- **Impact:** Loss of access to critical data
- **Likelihood:** Medium (based on recent sector-specific attacks)

6. Assess Likelihood and Impact

Use a simple matrix:



Example Scoring:

- Likelihood: High = 3
- Impact: High = 3
- Risk Score = 3 x 3 = 9 (Critical)

7. Document Everything in a Risk Register

Create a table with:

- Risk ID
- Asset
- Threat/Vulnerability
- Likelihood
- Impact
- Score
- Mitigation
- Status (Open, Accepted, Mitigated)

Sample Entry:

ID	Asset	Threat	Score	Mitigation
R01	HR Database	Insider Theft	9	Role-based Access
R02	Web Portal	SQL Injection	6	Input Validation

8. Involve Stakeholders

Meet with:

- IT and Infrastructure Teams
- Compliance and Legal
- Executives and Business Owners

Their feedback ensures the risk assessment reflects real-world priorities.

9. Prioritize Risks and Plan Mitigation

Not every risk can be eliminated. Choose from:

- **Avoid** – Stop the activity
- **Mitigate** – Add controls
- **Transfer** – Insurance or outsourcing
- **Accept** – Business agrees to bear the risk

10. Report Results Clearly

Tailor the final report to your audience. Include:

- Executive Summary
- Top Risks
- Recommended Actions
- Risk Heatmap
- Appendix with detailed risk register

Example Scenarios

Scenario 1: Outdated Web Server

Asset: Public-facing web server
Vulnerability: Apache version 2.4.29 with known CVEs
Threat: Remote code execution via crafted HTTP headers
Impact: Server takeover, reputational loss
Mitigation: Patch server, enable WAF, limit access

Scenario 2: Insecure Cloud Storage

Asset: AWS S3 bucket with sensitive logs
Vulnerability: Public read permissions enabled
Threat: Data exposure from web crawlers or malicious users
Impact: GDPR violation, data leakage
Mitigation: Apply least privilege policies, enable logging

Tools to Help You

- **Nessus** or **OpenVAS** – Vulnerability scanning
- **Threat Modeling Tool** – Microsoft Threat Modeling
- **Excel/Google Sheets** – Risk Register
- **RiskLens** – FAIR analysis platform
- **Lucidchart / draw.io** – Visualize assets and risks