Risk Assessment Process

What Is A Security Risk Assessment?

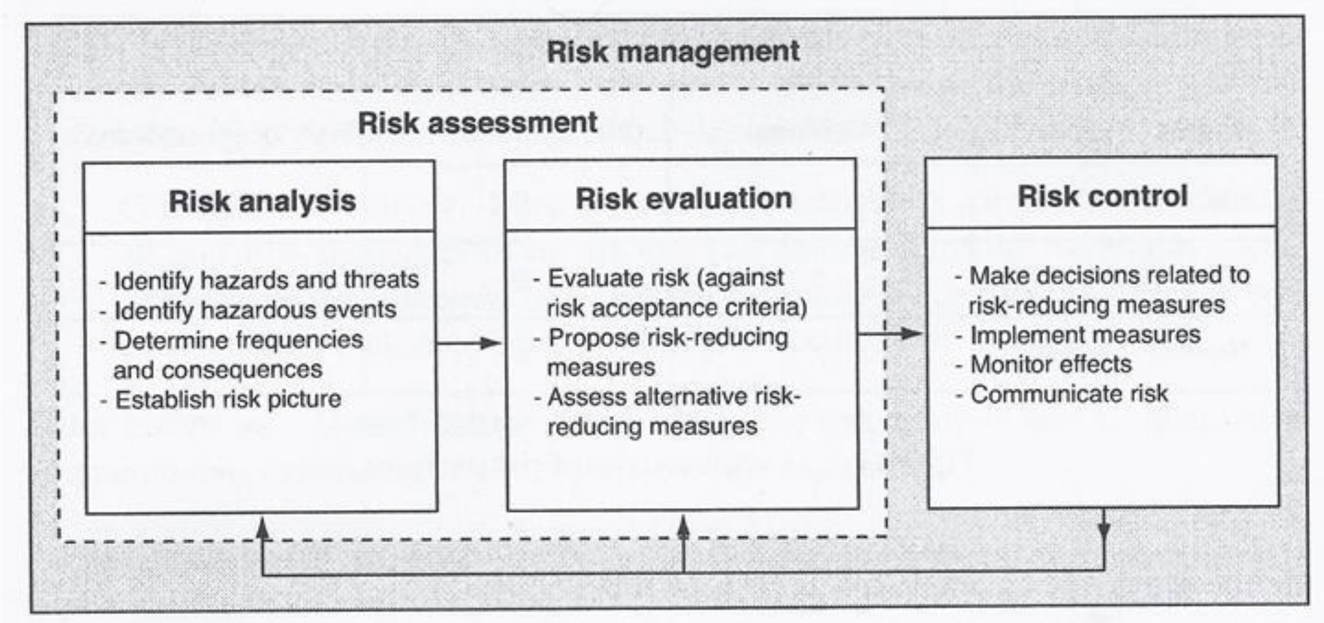
A security risk assessment is a process that identifies, evaluates, and prioritizes potential vulnerabilities to various information assets (i.e., systems, hardware, applications, and data) and then prioritizes the various risks that could affect those vulnerabilities.

- The primary purpose of a risk assessment is to inform decision-makers about vulnerabilities in corporate systems, allowing them to take preemptive defensive actions and prepare effective risk responses.

- The assessment also provides an executive summary to help executives make informed decisions about ongoing security efforts.

- Security risk assessments also indicate to management areas where employees need training to help minimize attack surfaces.

Risk Assessment VS Risk Management


Risk management
Risk assessment
Risk analysis
- Identify hazards and threats
- Identify hazardous events
- Determine frequencies and consequences
- Establish risk picture
Risk evaluation
- Evaluate risk (against risk acceptance criteria)
- Propose risk-reducing measures
- Assess alternative risk-reducing measures
Risk control
- Make decisions related to risk-reducing measures
- Implement measures
- Monitor effects
- Communicate risk

Why Are Security Risk Assessments Important?

- **Identify Security Gaps**
- **Reduce Long Term Costs**
- **Mitigate & Protect Against Breaches**
- **Help Budget Future Security Initiatives**
- **Increases Employee Security Awareness**

What Are The Different Types Of Security Risk Assessments?

1) **Physical Security Assessment**

    - How easy it for people to get physical access to your systems?
    - Do you have security at the entrances to the building?
    - Do you log visitors?
    - Are there security cameras in sensitive locations?
    - Do you have biometric locks on your server room?

2) **IT Security Assessment**

They identify broad system vulnerabilities that are not specific to particular applications or data storage facilities, as well as misconfiguration issues that frequently leave companies open to attack.

3) **Data Security Assessment**

- Is company data subject to least privilege and/or zero trust access controls?
- Do you use network segmentation to limit data access?
- Do you have strong identity management processes?
- Data security assessments consider the ease and breadth of access to corporate data.

4) **Application Security Assessment**

Application security assessments consider application vulnerabilities at every level from the code itself to who has access to the applications.

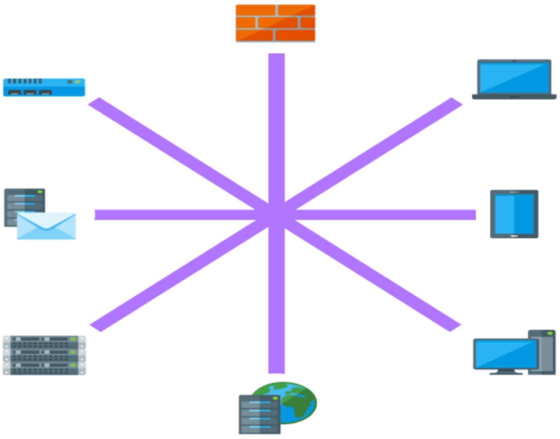
They allow companies to strengthen their applications and limit access to that needed for employees to perform their jobs.

5) **Insider Threat Assessment**

The 8 Step Security Risk Assessment Process

1. Map Your Assets
2. Identify Security Threats & Vulnerabilities
3. Determine & Prioritize Risks
4. Analyze & Develop Security Controls
5. Document Results From Risk Assessment Report
6. Create A Remediation Plan To Reduce Risks
7. Implement Recommendations
8. Evaluate Effectiveness & Repeat

Step 1: Map Your Assets



- Without a thorough understanding of your organization’s assets, security efforts will always be lacking.
- Therefore, the first step in any effective security risk assessment is to generate a complete map of potentially vulnerable assets.
- Asset maps require more than identifying hardware in use.
- You must also include all applications, all users (whether human or processes) and all data storage containers because each of these contributes to your overall attack surface.
- You should log and track each asset in a centralized database that you can quickly and easily update
- For users, you need to have a centralized system for assigning and managing all users and their respective permissions, for instance, an Active Directory system.
- After completing your asset inventory, you should assign each asset a value and map data flows among your various resources.
- Building data flow diagrams allows you to understand better where weak points and vulnerabilities exist in your network.
- As part of assigning value to your assets, you should categorize your data by access levels.

Example categories include:

- **Public** – Data that you intentionally make publicly available and that generates no concerns in the event of a breach.
- **Confidential** – Data that is not publicly accessible and that you only share with third parties under a non-disclosure agreement (NDA). Potentially includes sensitive technical, financial or customer information.
- **Internal Use Only** – The term is self-explanatory; this is information that you do not share outside the company, even with an NDA.
- **Intellectual Property** – This includes trade secrets and sensitive information underlying issued patents, pending patent applications and copyrights.
- **Compliance Restricted Data** – This includes any data subject to legal or regulatory obligations, such as HIPAA, GDPR, CMMC, for example.
- Data flow analyses should include what data is stored where and which users have access to what data. User is a generic term that can include any person, program or process with access to corporate data storage.
- In addition to identifying all internal assets, you must also identify and track connections to and data sharing with third-party providers, whether infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), software-as-a-service (SaaS), or other type of service provider.

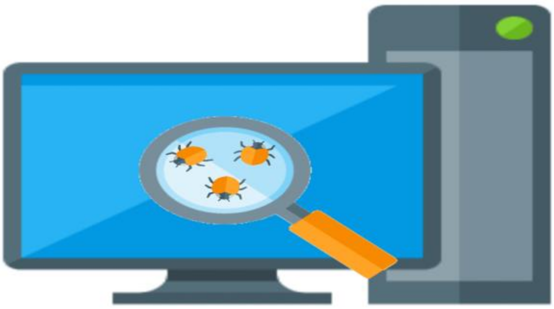
Third-party data flow assessments are particularly important for compliance with worldwide data privacy laws and regulations.

Building data flow maps, whether internal or with third-party providers, requires that you know:

- What data you have
- How you collect data (online forms, phone calls, hard copy, etc.)
- How you store data (electronic databases, hard copy documents, etc.)
- Where you store data (internal electronic storage, filing cabinets, cloud storage, backup hardware, etc.)

- How you process data (internal workflows)
- How you transfer data (email, FTP sites, phone, mail, etc.)

Step 2: Identify Security Threats & Vulnerabilities



Having built your asset inventory, you can now begin to identify vulnerabilities and threats for each asset.

There are many tests and risk assessment software tools available to help you in this process.

For example, vulnerability scanning investigates your network and applications to identify susceptibility to known threats.

Having scan results categorized by severity allows your security team to prioritize remediation efforts.

Security gap analyses compare your current state of security readiness to established standards, such as CIS Top 18, CMMC or PCI/DSS. These analyses help you identify administration and configuration risks.

Penetration testing takes vulnerability and threat assessment to the next level.

By replicating actual attacks on your systems, pen testing can both validate the results of your vulnerability scans and security gap analyses and pinpoint previously unidentified vulnerabilities.

Pen testing also tells you more than whether a vulnerability exists and can be exploited.

It lets you assess how difficult it is to access your systems, as well as the scope of access and potential damage from a successful attack.

You will calculate a risk rating for each vulnerability that indicates the likelihood and impact of an exploit.

For known vulnerabilities, public information will give you a good sense of how easy it is to exploit the vulnerability, including whether there are already public tools designed to exploit the vulnerability.

For other vulnerabilities, pen testing can help you determine the likelihood of an exploit.

You also want to assess the potential impacts for each vulnerability:

- Is the most likely outcome business disruption?
- Can attackers completely lock you out of your systems or permanently destroy data?
- Are you subject to fines for compliance violations?

Step 3: Determine & Prioritize Risks

- **Vulnerability and security threat assessments will invariably identify more risks than you can address at once.**
- **Therefore, when following your risk assessment procedures, your next step is to prioritize risks by giving each vulnerability a risk rating so that you can prepare your remediation plans.**

- **Prioritizing your remediation responses involves assessing your overall remediation budget against the risks and impacts of each threat or vulnerability.**
- **For example, you may decide to prioritize vulnerabilities that affect medium-value assets if the likelihood of exploit and damage potential is much more significant than for higher-value assets.**
- **Costing remediation efforts should include the costs of employees allocated to security efforts.**

Step 4: Analyze & Develop Security Controls

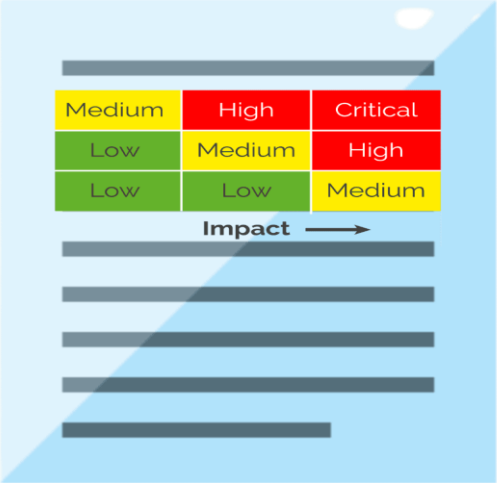
For any given vulnerability, there are several types of security controls you may consider.

The primary security controls are:

- Physical Security Controls – These control physical access to corporate assets and include biometric or coded locks, security cameras and guards, among other protections.
- Administrative Security Controls – These include corporate security policies, practices and workflows.

- Technical Security Controls – As the name suggests, these controls apply technological resources to address risk, including software tools such as firewalls, encryption and antivirus programs.

Step 5: Document Results From Risk Assessment Report



Medium	High	Critical
Low	Medium	High
Low	Low	Medium

- Effective risk assessment reports will condense the results of the various threat and vulnerability assessments in a concise threat ranking that show you a visual prioritization of your remediation plan.
- One effective way to represent your risk prioritization is using risk analysis templates, for example, a risk matrix.
- The risk matrix compares various levels of likelihood of exploitation against the severity of the damage from a successful attack.

Step 6: Create A Remediation Plan To Reduce Risks

Create A Remediation Plan To Reduce Risks - security risk assessment

Now that you have determined risk ratings and the order in which you will address vulnerabilities, you can begin creating your detailed vulnerability remediation plan.

This should include the basic, high-level steps for each remediation process and the associated costs.

If you still have several options for a given vulnerability, you should perform a cost/benefit analysis.

Comparing the cost of remediation against the potential cost of a successful attack can assist you in narrowing down to your preferred control.

Costs are not limited to monetary expenditures; they can also include the time it takes to implement a solution and the disruption to the business.

For example, applying software patches may have little overall cost for an organization, but it can be disruptive if done during business hours.

Step 7: Implement Recommendations

Implement Recommendations - security risk assessmentIt's finally time for action.
Your security team should now assign each item in the remediation plan to the appropriate team.

Assignments should include realistic time frames for completion.

In addition, you should indicate steps that teams should take to monitor the effectiveness of their remediation efforts, as well as any necessary reporting workflows.

As part of your remediation efforts, you should consider proactive risk responses such as Managed Detection and Response (MDR) solutions or Security Information and Event Management (SIEM) solutions.

Your choice among proactive risk response solutions may depend on whether you want to keep your efforts internal (SIEM) or whether you want to rely on external providers (MDR).

Experienced external providers can also help you build your SIEM processes, even if you control them internally.

Step 8: Evaluate Effectiveness & Repeat

Evaluate Effectiveness & Repeat - security risk assessment

Risk assessments are never static processes.

They require ongoing monitoring and optimization. As the old saying goes, rinse and repeat

Internal audits are one way to evaluate whether remediation efforts are working.