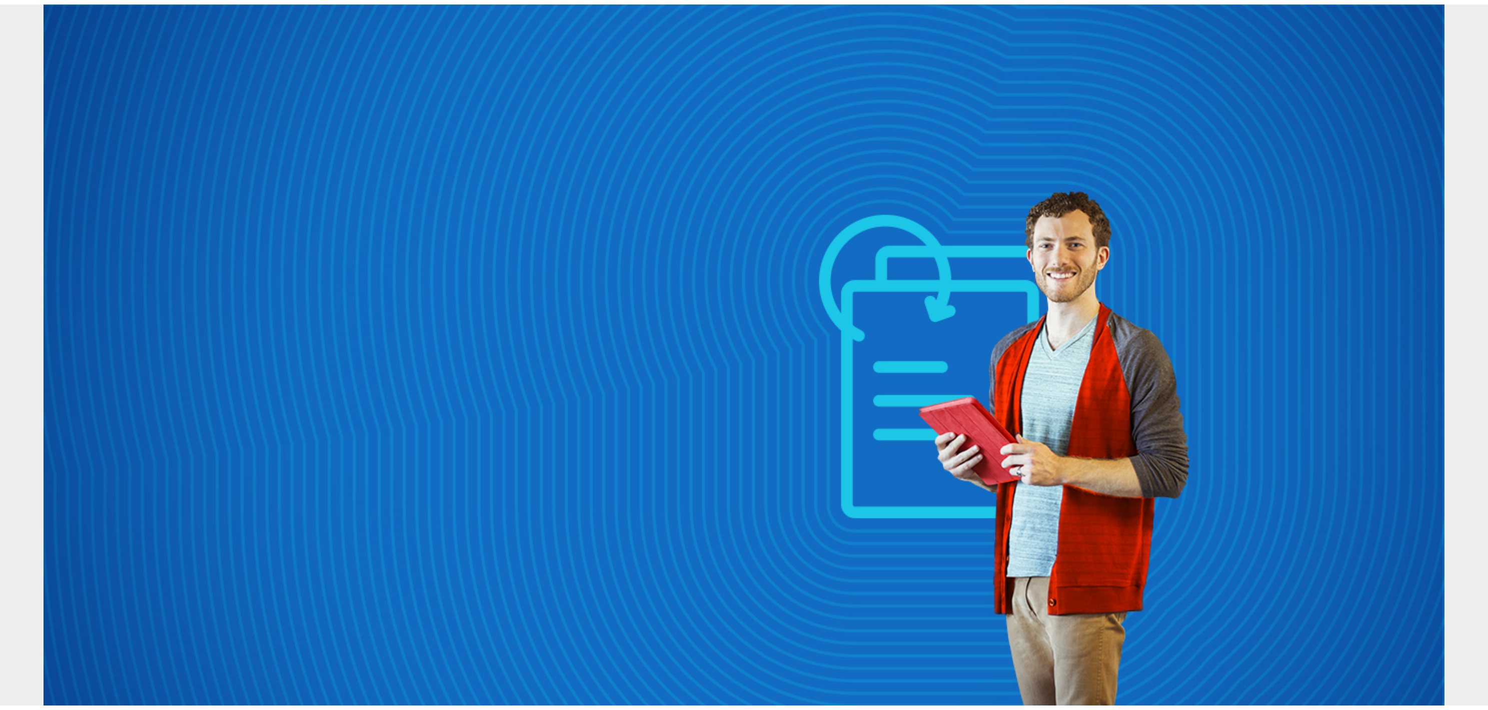
RISK ASSESSMENT VS VULNERABILITY ASSESSMENT: HOW TO USE BOTH



We've all heard the quote "Information is the lifeblood of an organization". Whenever I hear it, I am reminded of something I read:

To the modern business, data is the crucial fluid that carries nutrients (information) to those business functions that consume it.

The security of information has become a very critical activity in business, particularly considering digital transformation strategies and the advent of stricter data privacy regulation. Cyberattacks continue to be the biggest threat to organizational data and information; it is no surprise that the first step to countering these attacks is understanding the source and trying to nip the attack in the bud.

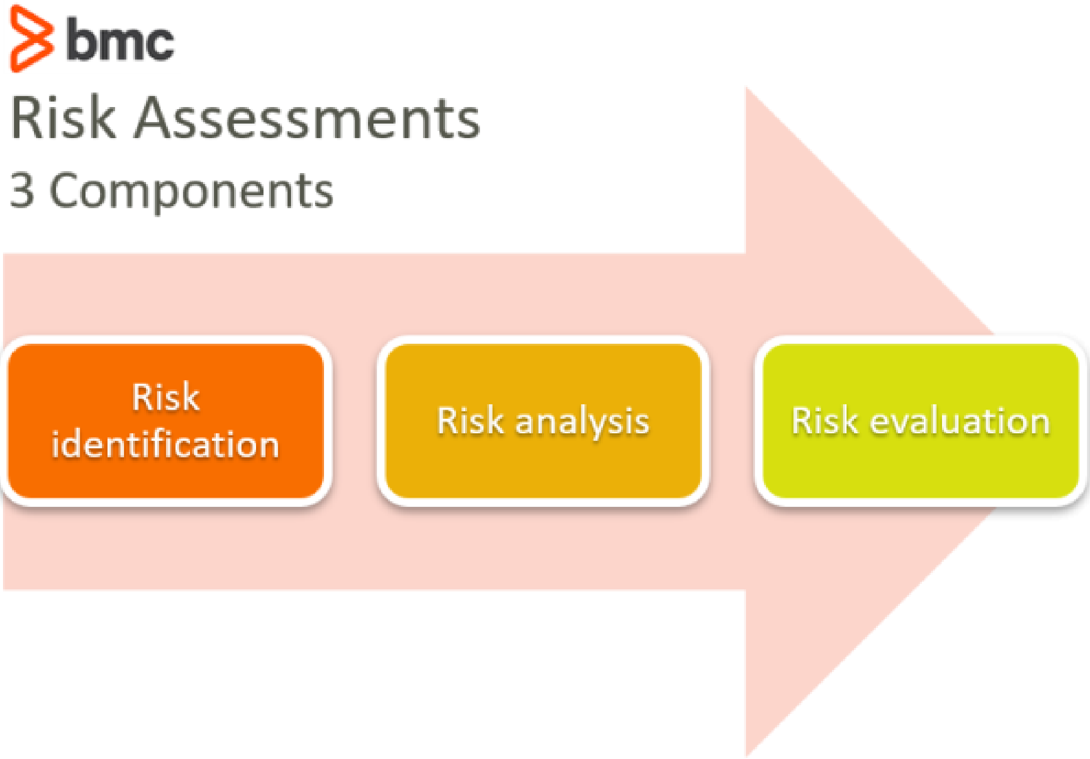
The two ways of understanding common threat sources in information security are risk assessments and vulnerability assessments. Both are indispensable in not only understanding where dangers to the confidentiality, integrity, and availability of information can come from, but also determining the most appropriate course of action in detecting, preventing, or countering them. Let's look at these assessments in detail.

(This article is part of our Security & Compliance Guide. Use the right-hand menu to navigate.)

Understanding risk assessments

First, let's clarify what we mean may risks. ISO defines risk as the "effect of uncertainty on objectives", which focuses on the effect of incomplete knowledge of events or circumstances on an organization's decision making. For an organization to be confident in its likelihood of meeting its goals and objectives, an enterprise risk management framework is required—the risk assessment.

Risk assessment, then, is a systematic process of evaluating the potential risks that may be involved in a projected activity or undertaking. In other words, risk assessment involves identifying, analyzing, and evaluating risks first in order to best determine the mitigation required.



Let's break down the three components of risk assessments:

1. Identification

Look critically at your organization's context in terms of sector, operational processes and assets, sources of risks, and the outcome should they materialize. For example, an insurance company might handle customer information in a cloud database. In this cloud environment, sources of risks might include ransomware attacks, and impact might include loss of business and litigation. Once you've identified risks, keep track of them in a risk log or registry.

2. Analysis

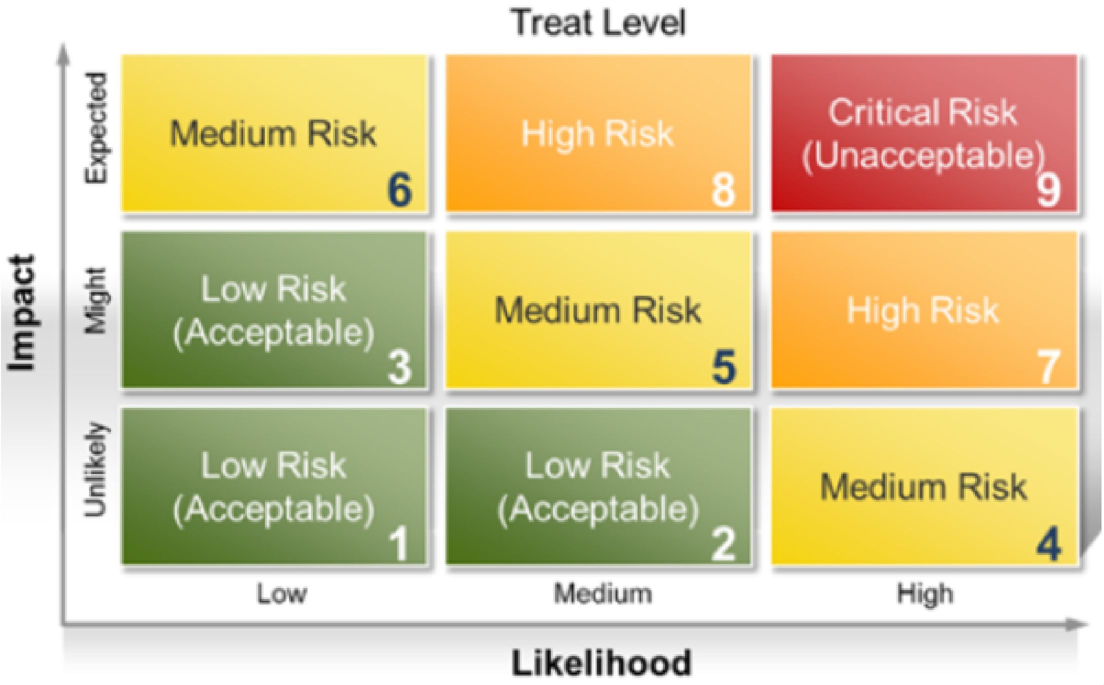
Here, you'll estimate the likelihood of the risk materializing as well as the scale of the impact to the organization. For example, a pandemic might have a low probability of occurring but a very high impact on employees and customers should it arise. Analysis can be qualitative (using scales, e.g. low, medium, or high) or quantitative (using numeric terms e.g. financial impact, percentage probability etc.)

3. Evaluation

In this phase, evaluate the results of your risk analysis with the documented risk acceptance criteria. Then, prioritize risks to ensure that investment is focused on the most important risks (see Figure 2 below). Prioritized risks might be ranked in a 3-band level, i.e.:

- Upper band for intolerable risks.

- Middle band where consequences and benefits balance.
- A lower band where risks are considered negligible.



Treat Level

Impact	Low	Medium	High
Expected	Medium Risk 6	High Risk 8	Critical Risk (Unacceptable) 9
Might	Low Risk (Acceptable) 3	Medium Risk 5	High Risk 7
Unlikely	Low Risk (Acceptable) 1	Low Risk (Acceptable) 2	Medium Risk 4

Likelihood

Figure 2: Risk Analysis and Evaluation Matrix

When to perform risk assessments

In an enterprise risk management framework, risk assessments would be carried out on a regular basis. Start with a comprehensive assessment, conducted once every three years. Then, monitor this assessment continuously and review it annually.

Risk assessment techniques

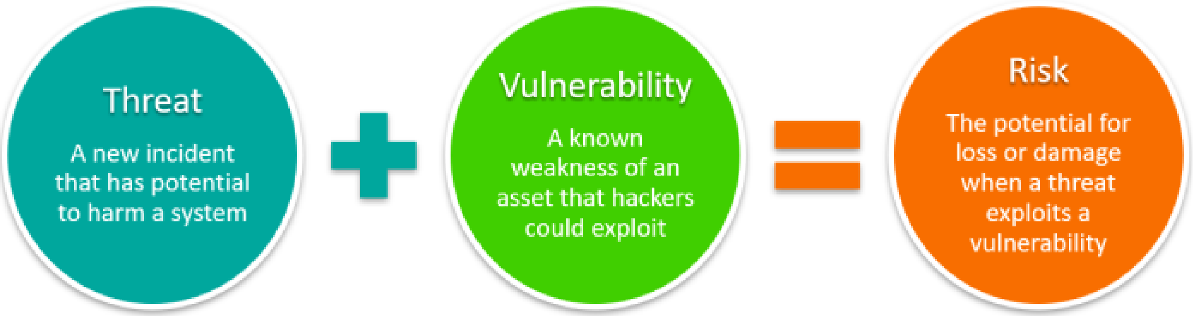
There are many techniques involved in risk assessments, ranging from simple to complex. The IEC 31010:2019 lists a few methods:

- Brainstorming
- Risk checklists
- Monte Carlo simulations

The decision on the technique should be driven by business needs and capabilities.

What are vulnerability assessments?

Understand your vulnerabilities is just as vital as risk assessment because vulnerabilities can lead to risks. The ISO/IEC 27000:2018 standard defines a vulnerability as a weakness of an asset or control that can be exploited by one or more threats. For example, an untrained employee or an unpatched employee might be thought of as a vulnerability since they can be compromised by a social engineering or malware threat. Research from Statista reveal that 80% of enterprise representatives believe their own employees and users are the weakest link in in their organization's data security.


Threat
A new incident that has potential to harm a system
Vulnerability
A known weakness of an asset that hackers could exploit
Risk
The potential for loss or damage when a threat exploits a vulnerability

How to conduct a vulnerability assessment

A vulnerability assessment involves a comprehensive scrutiny of an organization's business assets to determine gaps that an entity or event can take advantage of—resulting in the actualization of a threat. According to an article by Security Intelligence, there are four steps involved in vulnerability assessment:

1. **Initial Assessment.** Identify the organization's context and assets and define the risk and critical value for each business process and IT system.
2. **System Baseline Definition.** Gather information about the organization before the vulnerability assessment e.g., organizational structure, current configuration, software/hardware versions, etc.
3. **Vulnerability Scan.** Use available and approved tools and techniques to identify the vulnerabilities and attempt to exploit them. Penetration testing is one common method.
4. **Vulnerability Assessment Reporting.** Summarize your findings, including name and description of vulnerability, score, potential impact, and recommended mitigation.

Resources for vulnerability assessments

In information security, Common Vulnerabilities and Exposures (CVE) databases are the go-to resource for information on systems vulnerabilities. The most common databases include:

- The National Vulnerability Database (NDV)
- Mitre Corporation's CVE
- cvedetails.com

Penetration testing (or ethical hacking) usually takes advantage of vulnerability information from CVE databases. Unfortunately, there is no database on human vulnerabilities. Social engineering has remained one of the more prevalent cyber-attacks that takes advantage of this weakness where employees or users are untrained or unaware of threats to information security.

Common vulnerabilities in 2020

The Cybersecurity and Infrastructure Security Agency (CISA) recently provided guidance on the most commonly known vulnerabilities exploited by state, nonstate, and unattributed cyber actors in the last few years. The most affected products in 2020 include:

- Microsoft Office 365
- VPNs

- Weaknesses such as poor employee education
- Lack of system recovery and contingency plans

No surprises here, unfortunately. The most common interfaces to business information will be the most researched to identify gaps in security.

Assessing risks and vulnerabilities

It is clear that vulnerability assessment is a key input into risk assessment, so both exercises are crucial in securing an organization's information assets and increasing its likelihood of achieving its mission and objectives. Proper identification and addressing of vulnerabilities can go a long way towards reducing the probability and impact of threats materializing at system, human, or process levels. Performing one without the other, however, is leaving your company more exposed to the unknown.

It is important that regular vulnerability and risk assessments become a culture in every organization. A committed, ongoing capacity should be created and supported, so that everyone within the organization understands their role in supporting these key activities.

Additional resources

For more on vulnerability and risk assessments, browse the BMC Security & Compliance Blog or check out these articles:

- IT Risk Management & Governance
- 5 Steps to get Started with Risk Management
- IT Risk Assessment and ITSM Service Delivery: What You Need to Know
- Solving the Security Risk Your CISO Doesn't Know About
- Introduction to Information Security Management Systems (ISMS)