Risk Assessment vs Risk Analysis

Published April 4, 2022 • By Reciprocity • 7 min read

Although people often use the words “assess” and “analyze” interchangeably, the terms are not synonymous in risk management. Each one has a specific meaning, and the distinction between the two is important.

A risk assessment forms the backbone of your overall risk management plan. A risk analysis is one piece of the assessment process, where you determine the likelihood and criticality of each risk, and then assign each risk a score based on your findings. Just as we explain in our article on risk appetite versus risk tolerance, these are relevant terms you should review.

What is Risk?

Business risk is a threat to a company’s ability to meet its objectives. Put another way, risk refers to the fact that an organization’s ambitions may not work out as planned or that its objectives might go unmet.

external factors, including natural disasters, global pandemics, raw material prices, increased levels of competition, or changes to current government regulations.

What Is a Risk Assessment?

A risk assessment evaluates all the potential risks to your organization's ability to do business. These include project risks, enterprise risks, control risks, and inherent risks.
A risk assessment consists of two main parts: risk identification and risk analysis. Each component comprises several necessary actions.

In security, risk assessments identify and analyze external and internal threats to enterprise data integrity, confidentiality, and availability. This includes potential threats to information systems, devices, applications, and networks. A risk analysis is conducted for each identified risk, and security controls are pinpointed to mitigate or avoid these threats.

Security risk assessment models typically involve these elements:

- Identifying the organization's critical technology assets as well as the sensitive data those devices create, store, or transmit;
- Creating a risk profile for each asset;
- Assessing cybersecurity risks for all critical assets;
- Mapping all critical assets' interconnections;
- Prioritizing which assets to address after an IT security breach;
- Developing a mitigation plan with security controls for each risk;
- Preventing or minimizing attacks and vulnerabilities;
- Monitoring risks, threats, and vulnerabilities on an ongoing basis.

Security risk assessments are essential not just for cybersecurity but also for regulatory compliance. For example, the Health Information Portability and Accountability Act (HIPAA) requires periodic security risk assessments.

Publication 800-53, Guide for Conducting Risk Assessments, provides a framework for the information security risk assessment process.

Many organizations use risk management and compliance software to help them manage all the tasks associated with risk assessment, analysis, and management.

Security risks aren't the only type of risk that organizations face. Here are some others:

- Financial risk
- Audit risk
- Credit risk
- Compliance risk
- Reputational risk
- Competitive risk
- Legal risk
- Economic risk
- Operational risk
- Third-party risk
- Quality risk

What is the Risk Assessment Process?

Risk assessment happens in four steps.

1. Risk Identification

   Various types of hazards must be considered. Information security and cybersecurity risks often bubble to the top in a world connected with technology, uut you would be remiss if you only focused on technology-related risks. A risk register helps document and categorize the output from the risk identification process.

2. Determine Who and What Could Be Affected

possible outcomes. For example, what kinds of damages or injuries could result? Do they harm regulatory compliance? Who is at risk: employees, customers, other stakeholders? Each risk may pose a single threat or be dangerous in more ways than one.

3. Analyze Risks and Prevent Them

   After identifying the risks, it's time to perform the risk analysis and develop action plans. Assess the risk probability and criticality. Implement controls and risk response plans to prevent and mitigate risk.

   You are not expected to eliminate all risks since this is often not feasible. You should, however, take measures proportionate to the level of risk. This means that risks presenting a higher threat must receive more comprehensive control measures than lower-risk hazards. A risk matrix helps prioritize which risks need immediate attention.

4. Check the Risk Assessment

   Environments are ever-changing. Ensure risk assessments are reviewed periodically. They should always be inclusive of all potential risks and new risks.

What is a Risk Analysis?

Risk analysis is the phase where you'll examine each identified risk and assign it a score using one of two types of the scoring system: quantitative or qualitative. These scores help you prioritize your risks so you know which ones to address first and the best ways to address them.

Quantitative scoring assigns specific dollar amounts to the risk factors under consideration.

- What would be the cost to the organization if the risk were to happen? This is known as "single loss expectancy" (SLE).
- How often should you expect the risk to happen? Once per year assigns an annual rate of occurrence (ARO) of 1; once every 10 years, and ARO of 0.1.

Qualitative scoring is more subjective and uses a risk assessment matrix that typically involves four factors:

- **Likelihood:** What's the probability of occurrence: the probability that the risk will happen?
- **Impact:** If the risk event occurred, what is the impact of the risk? How much would it harm your project, function, or enterprise?
- **Velocity:** How quickly would your project, function, or enterprise feel the impact?
- **Materialization:** What's the potential severity of the impact? To measure this score, add the impact and velocity scores and divide by 2.

You can use mitigations or controls to reduce a risk's potential impact, velocity, and severity scores.

In the risk analysis phase, it's also essential to determine your organization's risk appetite and risk tolerance.

The COSO Enterprise Risk Management framework defines risk appetite as "the amount of risk, on a broad level, an organization is willing to accept in pursuit of stakeholder value."

Risk tolerance, the framework states, "reflects the acceptable variation in outcomes related to specific performance measures linked to objectives the entity seeks to achieve."

What is the Risk Analysis Process?

The risk analysis process entails the quantification of uncertainties. Estimating the potential impacts helps to develop the risk analysis framework. By employing risk analysis methods, action plans can be implemented to prevent, mitigate, or cope with risks.

1. Identification and Quantification of Uncertainties

its magnitude to the best of your knowledge. Identifying and quantifying uncertainties is a crucial step in risk analysis.

2. Estimation of Their Potential Impact

   It is necessary to estimate the impact of the various uncertainties. For instance, you may be unable to forecast the exact demand for your company's product; however, once you know our costs and margins, you can often estimate the impact on your net profit.

   Having done this, you can build a model that enables your organization to calculate the results for any given entry.

3. Development of a Risk Analysis Framework

   Once you perform these steps, your risk analysis model is set up. This model will have unknown inputs, uncertain variables, assumptions, or inputs.

   The model computes the outcomes for any particular input set of values. In contrast to other models, a risk analysis model requires you to think in ranks: Given that the entries are unknown and have many different values, the results are uncertain and may take on a wide range of values.

4. Formulation of Risk Management Actions

   Since a simulation of the risk management plan produces many potential values for the results you are interested in, it is essential to analyze the outcomes.

   For instance, we can synthesize the array of results using several types of statistics, such as the mean or median or the value at risk. Graphs and other risk management tools help visualize the results, such as frequency graphs and accumulated frequency graphs.

Identification: What's involved?

You'll need to use your imagination and envision worst-case scenarios for the risk identification phase, from natural disasters to economic ones.

secrets? What if the economy crashed? What if ransomware locked your systems? What if a competitor undercuts your prices?

During the risk identification process, it's essential to keep in mind that nobody can see into the future. New risks could emerge for which you have no plan (yet). Therefore, it's also essential to keep your options open and your risk management process and program flexible. Plan to review your risk list regularly and establish contingency plans for new risks.

So What's the Difference Between Risk Analysis and Assessment?

Risk assessment is considered the whole process where all types of risks are identified. Risk analysis is a step within the structure mentioned above, where each risk level is defined. Both are components within the larger whole known as risk management or risk evaluation.

It is essential to conduct various types of risk assessments to reveal all potential threats, whether they already exist or before they are generated.

It also generates a series of benefits such as avoiding data breaches, justifying the need for a cybersecurity program, cost-benefit analysis related to security risks, among others.

Prioritizing your Risks

Once you've assigned scores to your risks, you can categorize them according to their priority. For example, many enterprises allocate rankings of "high priority," "medium priority," or "low priority."

High Priority

A ransomware attack, in which malicious actors use malware to lock you out of your systems and demand payment to restore your access, would fall under this category. So would a zero-day attack, in which hackers exploit a previously unknown vulnerability.

A medium-risk event might be a former employee stealing information after being terminated. Reviewing your organization's employee-access policies would be a control against this risk's materializing. A robust employee termination process coordinated between human resources and IT would help mitigate this risk.

Low Priority

If your buildings are adequately secured, the probability might be low of someone's breaking into your offices and stealing devices. If those devices don't contain any information, the likelihood of a data loss may also be low or nil. Since there is no urgency associated with this risk, you might decide to review your device-risk-mitigation controls annually.

Manage Risk with ZenRisk

Keeping track of everything all at once and all the time can seem impossible, especially for cyber risk. Threat actors continually switch and evolve their tactics and technologies – and so must you, or risk losing control of your systems, data, and brand.

Instead of using spreadsheets for your risk management strategies, adopt Reciprocity ZenRisk to streamline evidence and audit management for all of your compliance frameworks. ZenRisk's risk and workflow management software is intuitive and simple to use.

ZenRisk helps you pinpoint risks by probing your systems and finding cybersecurity and compliance gaps. Then, it enables you to prioritize those risks and assign tasks to your team members. The user-friendly dashboards let you see the status of each risk and what needs to be done to address it.

Workflow management features offer easy tracking, automated reminders, and audit trails. The ZenConnect feature enables integration with popular tools, such as Jira, ServiceNow, and Slack, ensuring seamless adoption within your enterprise.

With ZenRisk, risk management takes care of itself – leaving you to other, more pressing concerns, like boosting your business and your bottom line.

Worry-free GRC is the Zen way. Schedule a demo now for your free consultation.