**What is risk management and why is it important?**

Risk management is the process of identifying, assessing and controlling threats to an organization's capital, earnings and operations. These risks stem from a variety of sources, including financial uncertainties, legal liabilities, technology issues, strategic management errors, accidents and natural disasters.

A successful risk management program helps an organization consider the full range of risks it faces. Risk management also examines the relationship between [different types of business risks](https://www.techtarget.com/searchcio/feature/4-basic-types-of-business-risks-in-the-enterprise) and the cascading impact they could have on an organization's strategic goal

Indeed, the aim of any risk management program is not to eliminate all risk but to preserve and add to overall enterprise value by making smart risk decisions.

Every organization faces the risk of unexpected, harmful events that can cost it money -- or, in the worst case, cause it to close.

"We don't manage risks so we can have no risk. We manage risks so we know which risks are worth taking, which ones will get us to our goal, which ones have enough of a payout to even take them," said Forrester Research senior analyst Alla Valente, who specializes in [governance, risk and compliance](https://www.techtarget.com/searchsecurity/definition/governance-risk-management-and-compliance-GRC) (GRC), third-party risk management, ERM and other risk-related topics.

Why is risk management important?

If an unforeseen event catches your organization unaware, the impact could be minor, such as a small impact on your overhead costs. In a worst-case scenario, though, it could be catastrophic and have serious ramifications, such as a significant financial burden or even the closure of your business.

To reduce risk, an organization needs to apply resources to minimize, monitor and control the impact of negative events while maximizing positive events. A consistent, systemic and integrated approach to risk management can help determine how best to identify, manage and mitigate significant risks.

The risk management process

At the broadest level, risk management is a system of people, processes and technology that enables an organization to establish objectives in line with values and risks.

A successful risk assessment program must meet legal, contractual, internal, social and ethical goals, as well as monitor new technology-related regulations. By focusing attention on risk and committing the necessary resources to control and mitigate risk, a business protects itself from uncertainty, reduce costs and increase the likelihood of business continuity and success.

The Five-Step Risk Management Lifecycle

How can you prevent a natural disaster or perfectly forecast customer demand for your products? You can’t. But the goal isn’t total risk prevention—it’s risk management. To succeed at risk management, you need to understand the full process and learn how to apply it to any scenario.

There are five phases in the risk management lifecycle.

1. Risk identification

First, you need to take stock of the threats your company faces. The specific risks will depend on your company and business processes, but there are several common classifications:

Operational risks specific to your industry, like the presence of heavy machinery or toxic chemicals

Weather-related risks like hurricanes, winter storms, or flooding

Legal or compliance risks (if you’re in a highly regulated industry)

Financial risks, such as poor cash flow management

To get the most comprehensive picture of your risk landscape, you’ll want to gather unique perspectives from across the organization. For example, say your company does long-haul trucking. Your drivers will have an acute sense of what can go wrong on the road but little visibility into office-side problems. Likewise, your logistics team will understand centralized risks but only have a vague sense of what drivers deal with.

2. Risk Analysis

Next, you'll analyze your identified risks. There are two key factors

to consider for each threat:

•

How likely is the threat to happen?

What's the negative impact if the threat occurs?

Risks scoring highly in both categories should be addressed first,

followed by less likely and/or lower-impact risks.

A good example of risk assessment is extreme weather. Most companies deal with it, be it hurricanes, tornadoes, or winter storms. And as [Jonathan Erdman](https://www.alertmedia.com/blog/weather-risk-management/), Senior Digital Meteorologist at the Weather Channel, points out, risk analysis is critical to proper preparation.

“Know the types of weather hazards that can affect your area and have a system in place to communicate and alert your employees about these hazards,” Erdman commented. “Ask yourself, how susceptible is your area to flash flooding? How susceptible is it to the occasional light snow? Austin [Texas] is a perfect example of this—you may get one snowfall every couple of years, but when it does happen, it’s big. So you also have to think about infrequent events that can have big impacts and plan accordingly.”

3. Risk mitigation planning

Once you understand the risks you face, you need to decide how to deal with them. Along with likelihood and impact, you need to understand your risk tolerance. If facing a hazard carries a significant reward, you’re more likely to tolerate the risk. But if there’s no reward, there’s no value in taking on the risk.

Based on impact, likelihood, and tolerance, you have four primary risk responses to choose from:

A close-up of a white background

Description automatically generated

Avoidance: In some cases, it makes sense to bypass a risk altogether by avoiding the situation

Transference: You can transfer or share certain risks, usually by getting insurance against a risk coming to fruition

Mitigation: The most common risk response is mitigation, in which you take measures to reduce the likelihood or potential impact

Acceptance: For highly unlikely risks with minimal impact, you can just accept the risk and deal with the consequences

4. Risk management implementation

After developing risk management plans, it’s time to implement them. Depending on the threat, there are a variety of [risk mitigation strategies](https://www.alertmedia.com/blog/risk-mitigation-strategies/) to consider:

Exercise risks by practicing for them in scenarios like [fire drills](https://www.alertmedia.com/blog/how-to-conduct-a-fire-drill-at-work/)

Challenge risks by allowing them to progress until the danger becomes unmanageable

Isolate risks by minimizing potential impact, as is common with firewalls and network architecture in the cybersecurity world

Buffer a risk by using more resources to prevent it, for example, by adding slack time to a schedule or having extra personnel on hand

Make a contingency plan for when your initial risk mitigation strategy falls short of its goal

5. Risk management review and tracking

Once your process is in motion, you need to monitor the risk to see how the situation unfolds and respond accordingly. Sometimes, this can be quick—an oncoming winter storm will be over in a matter of days. Other times, it can be an ongoing process, like monitoring the risk of theft in a retail environment. A few best practices for monitoring risks:

Document every aspect of the situation for review later

Develop metrics and key performance indicators to objectively measure how your mitigation strategies worked

Communicate with stakeholders throughout the process

If a situation goes worse than expected, alter plans as necessary—safety is always top priority

A [risk management plan](https://www.alertmedia.com/blog/risk-management-plan/) isn’t a one-time project. It’s a living document, which you’ll adjust to reflect changes in your company and the threats you face. To keep your risk management plans current, you should:

Conduct risk assessments periodically to identify new risks or changed threats

Analyze changes in the risk profiles and risk appetite based on lessons learned

Use [after-action reviews](https://www.alertmedia.com/blog/after-action-review/) to review how effective your response plans were

Refine your risk management plans and the metrics you use in your decision-making process

Schedule exercises to test your plans as appropriate

From extreme weather to political unrest to near-constant cyberattacks, your company may face a diverse range of threats on a given day. On top of that, the threat landscape is constantly shifting.

2024 Threat Outlook Report

Get expert insights on the critical events that shaped 2024 to better protect and prepare your business in the year ahead.

[GET THE REPORT](https://www.alertmedia.com/resources/annual-threat-outlook-report/)

For example, you might think the rise of remote work has reduced risks for companies. But as [Ontic CEO Lukas Quanstrom](https://www.alertmedia.com/podcast/protective-intelligence-identifying-risks/) notes, that’s not the case. “We get that a lot, that it must be a lot safer because no one’s really going into work anymore,” Quanstrom commented. “But really what’s happened is the threats have been pushed away from the office, which is actually a more secure location typically, and dispersed geographically due to COVID. So security teams are stretched to monitor hundreds of staff, maybe thousands, now spread across a wide patch of less-secure turf.”

So, how can you hope to tackle multiple threats, many of which are unseen and far-flung across various locations? Ad-hoc solutions might work in the short term. But to be effective and handle risks at scale, you need a structured and repeatable approach. That’s where the risk management lifecycle comes in.

What is the five-step risk management lifecycle and how can it help you [mitigate risks](https://www.alertmedia.com/blog/risk-mitigation/) in your organization? Read on to learn more.

Risk Management Fundamentals

Before diving into the risk management lifecycle, let’s get a few basics out of the way.

What is risk management?

Risk management is a process for identifying, understanding, and responding to hazards that could harm your company. The process encompasses risks of all sizes, both internal and external. From international war down to a simple tripping hazard, you can apply risk management principles to manage and minimize the impact on your people, assets, and operations.

Some of the most common types of risk include:

Financial risks, such as bad investments or unpaid invoices

[Operational risks](https://www.alertmedia.com/blog/operational-risk-examples/) like equipment failures or theft

Strategic risks, including market shifts or declining customer demand

Compliance risks, such as [OSHA violations](https://www.alertmedia.com/blog/osha-violations/) or discrimination lawsuits

Reputational risks that harm people’s opinion of your company

Global risk due to political unrest, cultural differences, or natural disasters

Getting a handle on everything can seem daunting. But ignoring it can have painful—and expensive—consequences in a crisis. For example, research from IBM found that companies with regularly-tested incident response plans spent an average of [$2.66 million](https://www.ibm.com/downloads/cas/3R8N1DZJ) less dealing with data breaches.

The Five-Step Risk Management Lifecycle

How can you prevent a natural disaster or perfectly forecast customer demand for your products? You can’t. But the goal isn’t total risk prevention—it’s risk management. To succeed at risk management, you need to understand the full process and learn how to apply it to any scenario.

There are five phases in the risk management lifecycle.

1. Risk identification

First, you need to take stock of the threats your company faces. The specific risks will depend on your company and business processes, but there are several common classifications:

Operational risks specific to your industry, like the presence of heavy machinery or toxic chemicals

Weather-related risks like hurricanes, winter storms, or flooding

Legal or compliance risks (if you’re in a highly regulated industry)

Financial risks, such as poor cash flow management

To get the most comprehensive picture of your risk landscape, you’ll want to gather unique perspectives from across the organization. For example, say your company does long-haul trucking. Your drivers will have an acute sense of what can go wrong on the road but little visibility into office-side problems. Likewise, your logistics team will understand centralized risks but only have a vague sense of what drivers deal with.

Download the Threat Assessment Template

Identify the threats that will have the biggest impact on your organization with this fill-in-the-blank template.

[GET THE TEMPLATE](https://www.alertmedia.com/resources/threat-assessment-template/)

2. Risk analysis

Next, you’ll analyze your identified risks. There are two key factors to consider for each threat:

How likely is the threat to happen?

What’s the negative impact if the threat occurs?

Risks scoring highly in both categories should be addressed first, followed by less likely and/or lower-impact risks.

A good example of risk assessment is extreme weather. Most companies deal with it, be it hurricanes, tornadoes, or winter storms. And as [Jonathan Erdman](https://www.alertmedia.com/blog/weather-risk-management/), Senior Digital Meteorologist at the Weather Channel, points out, risk analysis is critical to proper preparation.

“Know the types of weather hazards that can affect your area and have a system in place to communicate and alert your employees about these hazards,” Erdman commented. “Ask yourself, how susceptible is your area to flash flooding? How susceptible is it to the occasional light snow? Austin [Texas] is a perfect example of this—you may get one snowfall every couple of years, but when it does happen, it’s big. So you also have to think about infrequent events that can have big impacts and plan accordingly.”

3. Risk mitigation planning

Once you understand the risks you face, you need to decide how to deal with them. Along with likelihood and impact, you need to understand your risk tolerance. If facing a hazard carries a significant reward, you’re more likely to tolerate the risk. But if there’s no reward, there’s no value in taking on the risk.

Based on impact, likelihood, and tolerance, you have four primary risk responses to choose from:

Avoidance: In some cases, it makes sense to bypass a risk altogether by avoiding the situation

Transference: You can transfer or share certain risks, usually by getting insurance against a risk coming to fruition

Mitigation: The most common risk response is mitigation, in which you take measures to reduce the likelihood or potential impact

Acceptance: For highly unlikely risks with minimal impact, you can just accept the risk and deal with the consequences

4. Risk management implementation

After developing risk management plans, it’s time to implement them. Depending on the threat, there are a variety of [risk mitigation strategies](https://www.alertmedia.com/blog/risk-mitigation-strategies/) to consider:

Exercise risks by practicing for them in scenarios like [fire drills](https://www.alertmedia.com/blog/how-to-conduct-a-fire-drill-at-work/)

Challenge risks by allowing them to progress until the danger becomes unmanageable

Isolate risks by minimizing potential impact, as is common with firewalls and network architecture in the cybersecurity world

Buffer a risk by using more resources to prevent it, for example, by adding slack time to a schedule or having extra personnel on hand

Make a contingency plan for when your initial risk mitigation strategy falls short of its goal

5. Risk management review and tracking

Once your process is in motion, you need to monitor the risk to see how the situation unfolds and respond accordingly. Sometimes, this can be quick—an oncoming winter storm will be over in a matter of days. Other times, it can be an ongoing process, like monitoring the risk of theft in a retail environment. A few best practices for monitoring risks:

Document every aspect of the situation for review later

Develop metrics and key performance indicators to objectively measure how your mitigation strategies worked

Communicate with stakeholders throughout the process

If a situation goes worse than expected, alter plans as necessary—safety is always top priority

A [risk management plan](https://www.alertmedia.com/blog/risk-management-plan/) isn’t a one-time project. It’s a living document, which you’ll adjust to reflect changes in your company and the threats you face. To keep your risk management plans current, you should:

Conduct risk assessments periodically to identify new risks or changed threats

Analyze changes in the risk profiles and risk appetite based on lessons learned

Use [after-action reviews](https://www.alertmedia.com/blog/after-action-review/) to review how effective your response plans were

Refine your risk management plans and the metrics you use in your decision-making process

Schedule exercises to test your plans as appropriate

Use this template to build a comprehensive risk mitigation plan.

GET THE TEMPLATE

Benefits of an Effective Risk Management Process

Risk management is a win in and of itself. You get a better handle on the risks you face and—hopefully—develop plans to avoid them. Also, risk management can have a positive ripple effect throughout your organization.

Improved business resilience

With thorough risk management plans, you can minimize disruptions to your business. And when things do go awry, you’ll be better positioned to get back up to speed quickly.

Safer work environment

Understanding your workplace risks allows you to prepare your team members to deal with them better. Through communication and training, you can prevent threats from materializing and keep your employees safe.

Competitive advantage

Effective risk management gives your company a leg up against competitors. Vendors and clients are more likely to do business with resilient operations, and employees want to work at a company that puts safety first.

Challenges in Managing Risk

Here are three common challenges to watch for in your risk management process.

Static plans for dynamic risks

Your business moves quickly. You’re moving assets around, swapping equipment, starting new projects, and constantly evolving. During fast-paced operations, it can be easy to let risk management plans slip out of date.

There are a few ways you can avoid this:

Make risk management part of your project management methodology

Perform periodic [infrastructure risk assessments](https://www.alertmedia.com/blog/infrastructure-risk-assessment/) to ensure they’re up to date

Schedule comprehensive risk management plan reviews to keep details from slipping through the cracks

Organizational gaps and siloed risk

Poor communication between departments is never good. But when it comes to risk management, it can lead to two critical problems:

Organizational gaps, where multiple parties think someone else is addressing an issue, but no one actually is

Siloed risks that only a select few people are aware of, leading to incomplete risk management strategies

Prevent gaps and silos by taking a top-down approach and engaging stakeholders throughout your organization. By making everyone a part of the risk management process, you’ll keep your team members in sync and protect your company.

Regulatory compliance

For some businesses, risk management planning isn’t just nice to have—it’s a requirement. Many industries must follow strict risk management guidelines from OSHA, seek ISO certification, or work with other regulatory agencies. And sometimes, each set of requirements can be slightly different.

Be sure to thoroughly view relevant regulations before you start the risk management process. Making a mistake can lead to fines or costly remediation efforts.

What is risk management?

Risk management is the process of identifying, assessing and controlling financial, legal, strategic and security risks to an organization’s capital and earnings. These [threats](https://www.ibm.com/threat-detection-response), or risks, could stem from a wide variety of sources, including financial uncertainty, legal liabilities, strategic management errors, accidents and natural disasters.

Why is risk management important?

If an unforeseen event catches your organization unaware, the impact could be minor, such as a small impact on your overhead costs. In a worst-case scenario, though, it could be catastrophic and have serious ramifications, such as a significant financial burden or even the closure of your business.

To reduce risk, an organization needs to apply resources to minimize, monitor and control the impact of negative events while maximizing positive events. A consistent, systemic and integrated approach to risk management can help determine how best to identify, manage and mitigate significant risks.

ReportCost of a Data Breach

Get insights to better manage the risk of a data breach with the latest Cost of a Data Breach report.

Related content

Register for the X-Force Threat Intelligence Index

The risk management process

At the broadest level, risk management is a system of people, processes and technology that enables an organization to establish objectives in line with values and risks.

A successful risk assessment program must meet legal, contractual, internal, social and ethical goals, as well as monitor new technology-related regulations. By focusing attention on risk and committing the necessary resources to control and mitigate risk, a business protects itself from uncertainty, reduce costs and increase the likelihood of business continuity and success.

Three important steps of the risk management process are risk identification, risk analysis and assessment, and risk mitigation and monitoring.

Identifying risks

Risk identification is the process of identifying and assessing threats to an organization, its operations and its workforce. For example, risk identification can include assessing IT security threats such as malware and ransomware, accidents, natural disasters and other potentially harmful events that could disrupt business operations.

Risk analysis and assessment

Risk analysis involves establishing the probability that a risk event might occur and the potential outcome of each event. Risk evaluation compares the magnitude of each risk and ranks them according to prominence and consequence.

Risk mitigation and monitoring

Risk mitigation refers to the process of planning and developing methods and options to reduce threats to project objectives. A project team might implement risk mitigation strategies to identify, monitor and evaluate risks and consequences inherent to completing a specific project, such as new product creation. Risk mitigation also includes the actions put into place to deal with issues and effects of those issues regarding a project.

Risk management is a nonstop process that adapts and changes over time. Repeating and continually monitoring the processes can help assure maximum coverage of known and unknown risks.

Risk response strategies and treatment

There are five commonly accepted strategies for addressing risk. The process begins with an initial consideration of risk avoidance then proceeds to 3 additional avenues of addressing risk (transfer, spreading and reduction). Ideally, these three avenues are employed in concert with one another as part of a comprehensive strategy. Some residual risk may remain.

What are the most common responses to risk?

Risk avoidance

Avoidance is a method for mitigating risk by not participating in activities that may negatively affect the organization. Not making an investment or starting a product line are examples of such activities as they avoid the risk of loss.

Risk reduction

This method of risk management attempts to minimize the loss, rather than completely eliminate it. While accepting the risk, it stays focused on keeping the loss contained and preventing it from spreading. An example of this in health insurance is preventive care.

Risk sharing

When risks are shared, the possibility of loss is transferred from the individual to the group. A corporation is a good example of risk sharing—several investors pool their capital and each only bears a portion of the risk that the enterprise may fail.

Transferring risk

Contractually transferring a risk to a third-party, such as, insurance to cover possible property damage or injury shifts the risks associated with the property from the owner to the insurance company.

Risk acceptance and retention

After all risk sharing, risk transfer and risk reduction measures have been implemented, some risk will remain since it is virtually impossible to eliminate all risk (except through risk avoidance). This is called residual risk.

https://technologyadvice.com/blog/information-technology/project-risks-examples/