

Provided by: McGriff

Creating a Risk Assessment Plan

All businesses face inherent risk, regardless of size and sector. While certain risks (e.g., entering new markets and launching new products) are critical for business growth, others (e.g., cyberattacks, natural disasters and supply chain disruptions) can hinder progress, cause financial losses and create legal liability. In some cases, a single disruptive event could even put a business at risk of insolvency. As such, managing risk is a core priority, particularly as organizations continue to face evolving threats, including those arising from disruptive technologies and an increasingly complex regulatory environment.

Fortunately, a comprehensive risk assessment plan can help organizations identify and assess potential risks, prioritize resources and respond proactively, reducing exposure and minimizing potential impacts.

This article outlines what a risk assessment plan is and explores how to build one.

What Is a Risk Assessment Plan?

A risk assessment plan is a strategic framework that outlines how an organization identifies, evaluates and manages risks. It facilitates effective decision-making and helps ensure consistency across the company.

At a high level, a well-constructed plan defines the scope of risks to be considered, outlines how they will be evaluated and clarifies roles, responsibilities and processes for ongoing review. It is typically aligned with broader organizational frameworks, such as enterprise risk management programs and health and safety systems, helping ensure a coordinated approach to risk and supporting compliance efforts.

Overall, a risk assessment plan provides a structured, organizationwide approach to risk, helping ensure potential threats are managed systematically rather than ad hoc.

How to Create a Risk Assessment Plan

The following seven steps provide a practical framework for developing a risk assessment plan:

- **Define the purpose and scope.** Organizations should define the plan's objectives, as well as the business activities, processes and departments that will fall within its scope. These should align closely with any regulatory and contractual obligations. Employers may choose to apply the plan across the entire organization or begin with higher-risk areas and activities, expanding the scope in phases. Early on, organizations should establish their risk tolerance, as some risks may not warrant inclusion if the potential for harm is low and the cost of prevention is high.
- **Establish risk assessment methodology.** Organizations should define the methods they will use to identify, analyze and prioritize risk, and establish clear risk categories (e.g., safety, operational, financial and compliance). Risk rating criteria and scoring methodologies should be designed to reflect the organization's size, industry and risk profile, taking into account factors such as risk likelihood, impact and severity. Organizations may use qualitative methods—which rely on expert judgment, risk scoring and risk matrices to assess risks based on likelihood and impact—or quantitative methods, which use

data, statistical analysis and cost-benefit analysis to assign numerical or financial values to risks. Many organizations begin with qualitative assessments and incorporate quantitative methods as their risk management program matures. Applying a consistent methodology can help organizations compare results across departments and prioritize resources more effectively.

- **Identify stakeholders and resources.** Organizations should identify key participants, including subject-matter experts and leadership-level decision-makers. Representation from across the organization (e.g., finance, IT and operations) can help ensure a well-rounded understanding of risk, as can engaging external stakeholders such as clients, suppliers and business partners. Organizations should also determine the resources required to support the process, including staff time, available budget, and any tools or systems needed.
- **Assign roles and responsibilities.** Organizations should clearly define responsibility for each aspect of the risk assessment process, including owning specific risks, leading risk assessments, approving findings and implementing corrective actions. They should also determine escalation procedures, specifying when risks require escalation to senior leadership. Clear accountability ensures risks are actively managed and that risk mitigation actions are implemented promptly.
- **Develop the assessment schedule.** Organizations should document how and when they will conduct risk assessments, including any key milestones and reporting deadlines. Time frames should align with regulatory expectations and account for the level of risk involved. For instance, higher-risk activities may require more frequent review due to their potential severity and impact. Organizations should also identify scenarios that may trigger an unscheduled review, such as workplace accidents, external audits, regulatory updates or significant operational changes.
- **Define documentation and reporting requirements.** Organizations should define how they document and report risk across the company to support consistency and provide evidence of decision-making in the event of a claim or investigation. This may include establishing standard templates and formats for recording risk assessments and maintaining a centralized risk register. Organizations should also define how they communicate findings, who conducts reviews and how long they retain risk assessment documentation.
- **Establish review and continuous improvement processes.** Organizations should track performance metrics (e.g., incident frequency, risk assessment completion rates and timely completion of mitigation actions) to ensure the plan is functioning as intended. They should also periodically review the plan to account for emerging risks and incorporate any lessons learned from incidents, audits and risk assessments.

Common Mistakes to Avoid

Risk assessment plans may fail to meet their objectives if they fall short in key areas. For example, unclear objectives or a poorly defined methodology can result in individuals across departments assessing risks differently, making it difficult to compare results and prioritize resources; poorly defined roles and responsibilities may mean individuals do not take ownership of risks, delaying action and allowing problems to escalate; and gaps in documentation or unrealistic assessment schedules may lead to missed or rushed assessments, increasing the likelihood that risks go unaddressed.

Organizations can minimize their exposure by ensuring their risk assessment plan is clearly defined, consistently applied, and regularly reviewed to reflect evolving risks and priorities.

Conclusion

Organizations face a wide range of internal and external risks that evolve over time. However, a well-developed risk assessment plan can help organizations identify and control potential threats, reduce exposure and support operational resilience.

Contact us today for additional risk management guidance.

This Risk Insights is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice. © 2026 Zywave, Inc. All rights reserved.