RISK & RESILIENCE

Enterprise Risk Management

Getting Started Guide

HUB

Risk & Insurance | Employee Benefits | Retirement & Private Wealth

Enterprise Risk Management: Getting Started

Organizations face a wide range of strategic, operational, financial and external risks that can affect their ability to achieve objectives. While risk cannot be entirely eliminated, an effective enterprise risk management (ERM) strategy enables companies to systematically identify, assess and prioritize risks, permitting them to make informed decisions about which risks to retain and how to manage them effectively.

This guide is designed to help entities that are starting, strengthening or benchmarking their risk management practices. Because every organization is unique, an effective strategy begins with understanding the current state of risk management within your organization. A clear baseline makes it easier to set practical goals and chart a path toward a more mature and resilient ERM framework.

Enterprise risk management principles

ERM is a disciplined, organization-wide practice that systematically uncovers, evaluates and helps prepare a full range of internal and external risks that could influence an organization's ability to pursue its goals. It brings together risk information from across functions and decision-makers to form a unified understanding of potential threats and opportunities, guiding leaders to make better-informed strategic choices, strengthen resilience and allocate resources where they matter most.

An effective ERM strategy enables organizations to:

- Develop an enterprise-wide view of risk by identifying, assessing and prioritizing the risks that most affect strategy, performance and resilience.
- Align risk appetite, escalation thresholds and governance with strategic planning, compliance and decision-making processes.
- Proactively identify emerging and high-impact risks to reduce volatility and support more informed, forward-looking leadership decisions.
- Establish consistent risk management processes with clear ownership, accountability and documented mitigation plans.
- Enhance transparency and confidence among stakeholders and regulators through meaningful risk reporting, oversight and ongoing monitoring.

Today's business environment presents both challenges and potential advantages. Effective ERM encourages leaders to balance risk mitigation with thoughtful risk-taking to support innovation and resilience. Doing so requires a comprehensive understanding of the strategic, financial, operational, legal, compliance and technology risks that influence business performance.

An enterprise risk assessment is a first step to setting priorities and establishing a risk register that can be updated as conditions evolve.

Strategic risks

Customers, competitors and investors

An ERM strategy should evaluate how risks may influence your mission and strategy. Strategic risks can disrupt an organization's ability to achieve its goals and adapt to a changing environment. Because these risks directly affect performance and competitive standing, they require a different approach than operational or compliance risks.

While it's appropriate to avoid or prevent certain risks, strategic risks often involve calculated choices — such as entering new markets, developing new products or evaluating acquisitions — that may ultimately create value. An ERM framework helps leaders evaluate these decisions with a clearer understanding of potential impacts.

Financial risks

Market and economic change

A comprehensive ERM program includes an assessment of financial risks and exposures, both at the micro- and macroeconomic level, affecting key financial controls as well as reporting processes. These risks may involve interest rate shifts, currency exposure and commodity fluctuations.

Understanding the stability and reliability of key accounts, transactions and controls is essential. This analysis supports more informed planning, reporting and risk mitigation efforts.

Legal and compliance risks

Law, regulation, politics and corporate governance

Legal and compliance risks should be identified and monitored as part of the ERM strategy. This includes evaluating regulatory requirements, corporate governance and cultural factors that influence behavior.

A strong compliance culture helps protect your organization and supports long-term performance. Embedding ethical behavior within the enterprise can drive business results and proactively manage compliance risk. Because regulations continue to evolve, an ERM program should account for emerging requirements and the potential implications of noncompliance.

Operational risks

Processes, systems, people and supply chain

Operational risks arise from day-to-day activities and may involve processes, people, technology or supply chain dependencies. Assessing these risks helps determine where vulnerabilities could affect business continuity or performance.

An ERM framework supports a structured way to identify these risks, evaluate their impacts and prioritize controls or improvements — whether internal or related to third-party partners and vendors.

IT and systems risks

Hardware, software and network controls

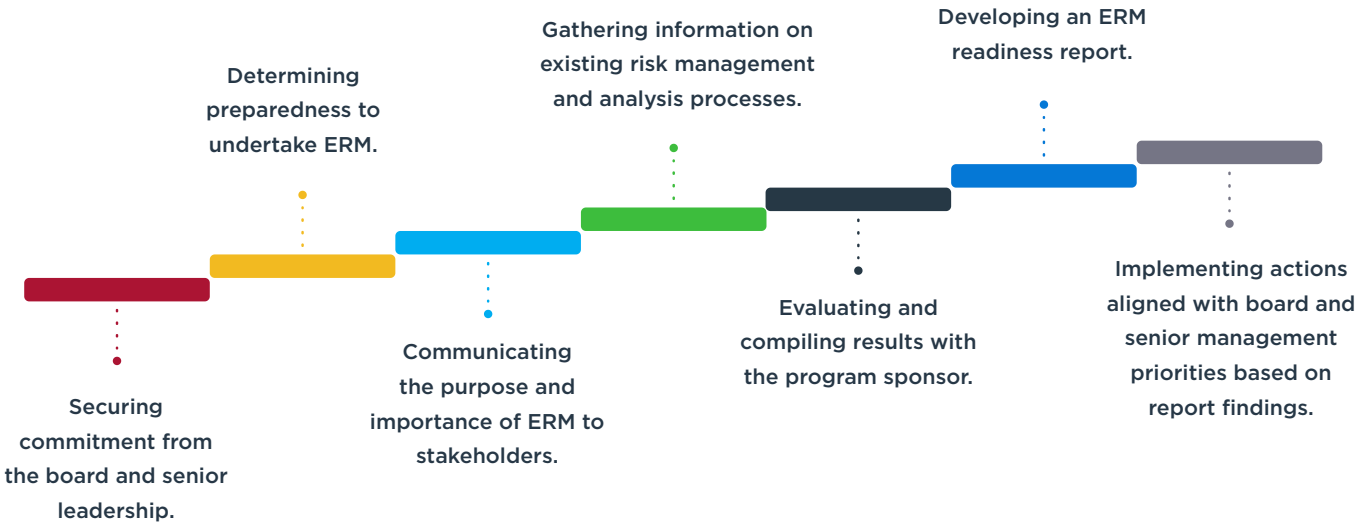
Technology-related risks encompass infrastructure, cybersecurity, data privacy and the potential for system failures or service disruptions. An ERM strategy should assess both current capabilities and areas where innovation or modernization may be needed.

Understanding these risks allows organizations to protect critical systems, safeguard sensitive information and maintain reliable operations.

Putting ERM into action

Effective risk management is constant discipline, not a one-time exercise. As organizations evolve, so do the risks they face — making it essential to regularly reassess exposures, refine mitigation plans and align risk strategies with broader business objectives. A thoughtful, well-structured ERM framework strengthens resilience and supports better decision-making, improved governance and long-term stability.

A project roadmap for ERM will require:



By applying the principles and practices outlined in this guide, your organization can build a confident, proactive risk management strategy.

Whether you're looking to enhance your current risk management strategy or build a program from the ground up, our experts are ready to help. Get started with a **HUB ERM specialist** today.

Additional Resources

The following established bodies of knowledge offer valuable ERM guidance:

- **ISO 31000 Risk Management** – An international standard that provides principles, a framework and a process for managing risk in a structured and consistent way across any type of organization.
- **Committee of Sponsoring Organizations of the Treadway Commission (COSO)** – Offers information about the COSO ERM Framework and how to apply enterprise risk management by integrating strategy with performance.
- **RIMS Strategic and Enterprise Risk Center** – Provides risk professionals with knowledge, tools and resources to support strategic and enterprise risk management (SERM) efforts.
- **The Risk Maturity Model** – A resource for risk and governance professionals to aid in planning, implementing and maturing enterprise risk management practices.

Strategic support that puts you in control.

When you partner with us, you're at the center of a vast network of experts who will help you reach your goals. With HUB, you have peace of mind that what matters most to you will be protected — through unrelenting advocacy and tailored solutions that put you in control.

For more information on strategic enterprise risk management, contact a HUB ERM specialist.

hubinternational.com/erm

Ready for tomorrow.

Risk & Insurance | Employee Benefits | Retirement & Private Wealth

HUB