BACK | NEXT

ENTERPRISE RISK MANAGEMENT
A handbook

VIEW THE DOCUMENT

Enterprise risk management: A 30,000-foot overview

Risk management and preparedness have always been critical for organizations, but the reality is, many organizations don't start thinking seriously about risk until it's too late. Unfortunately, when disasters like a pandemic or economic downturn strike, leaders of organizations of all types find themselves asking the same questions:

- *How could I have been better prepared to soften the blow?*
- *Where are the greatest risks in my organization right now?*
- *Which areas are especially vulnerable?*
- *What steps should I take to prepare for a future disaster?*

Don't look back in the midst of crisis and wonder — it's imperative to integrate enterprise risk management (ERM) into all activities across your organization.

What is ERM?

According to the **Committee of Sponsoring Organizations of the Treadway Commission (COSO),** ERM is defined as "the culture, capabilities, and practices integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value."

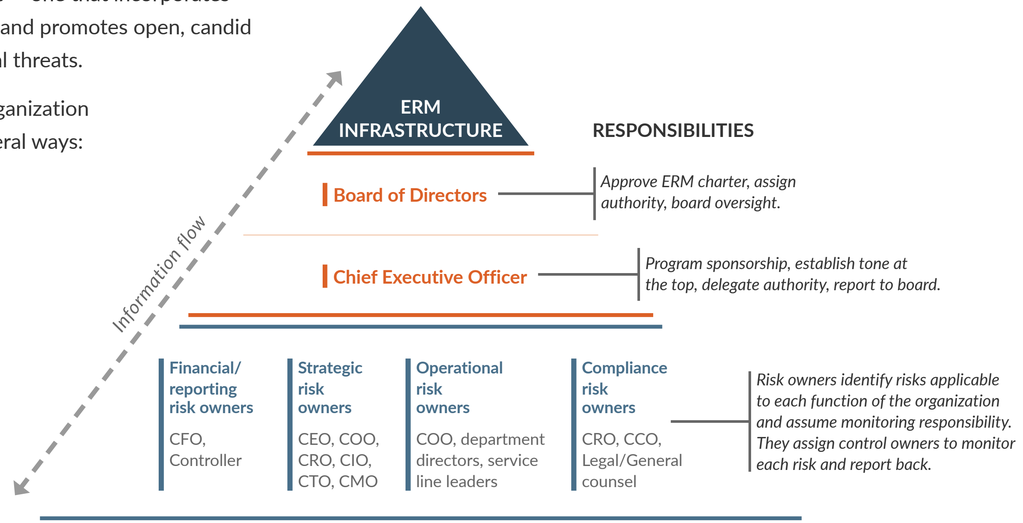
ERM isn't a once-and-done task. It's a continuous process that impacts all aspects of your organization and protects you from risks that threaten your strategic and operational objectives. A successful ERM framework depends on a shift in mindset — one that incorporates risk considerations into decision-making and promotes open, candid communication to stay ahead of potential threats.

In practice, applying ERM within your organization includes a focus on managing risk in several ways:

- *Fostering a risk-conscious culture*
- *Developing capabilities*
- *Applying practices*
- *Integrating risk considerations with strategy-setting & performance*
- *Managing risk to strategy & business objectives*
- *Linking to value*

ERM infrastructure is a key element of this discipline. The ability to quickly understand the likelihood and magnitude of a risk event before or at inception combined with the practiced deployment of risk management resources are critical to organizational longevity. Companies should prioritize ERM activities by deploying a framework that addresses — and protects — key elements of the organization:

Strategy setting, operations, compliance with regulation and law, as well as financial health and stability.



ERM IS DEFINED AS

"the culture, capabilities, and practices integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value."

ERM value proposition

All entities exist to provide value for stakeholders, and all entities face risk when pursuing value. ERM applies to all organizations, public and private, with principles applied consistently regardless of organizational structure. Integrating ERM practices throughout an organization improves decision-making in governance, strategy, objective-setting, and daily operations. It helps to enhance performance by more closely linking strategy and business objectives to risk. The diligence required to integrate enterprise risk management provides an entity with a clear path to creating, preserving, and realizing value.

Key aspects of ERM

Let's look more specifically at four key pillars of ERM that successful organizations consider when implementing an ERM framework.

1 PROCESS MANAGEMENT AROUND NEW AND EVOLVING RISKS

Organizational risks are growing more complex as companies evolve and new threats continue to emerge. Effective ERM alleviates the impact of ever-changing risk within organizations. Through the ERM process, an organization develops the capabilities to effectively adapt in an environment of change, enhancing enterprise resilience.

2 PREPAREDNESS FOR UNEXPECTED DISASTERS

The most unpredictable aspects of risks are timing and magnitude of a risk event. When ERM is integrated into operations, the organization is better able to identify key risk indicators and proactively manage the effects of an event, including both known and unknown circumstances.

> *All entities exist to provide value for stakeholders, and all entities face risk when pursuing value.*

> *Through the ERM process, an organization develops the capabilities to effectively adapt in an environment of change, enhancing enterprise resilience.*

3 STAFF ROLES AND ACCOUNTABILITY

Integrating ERM into an organization is a continuous, structured process that relies on multiple stakeholders. A successful ERM framework is designed to ensure stakeholders are doing their part to think critically about risk management. Emphasis always remains on continuous improvement of ERM practices, so the organization should have formal processes in place to ensure it's able to fulfill ERM responsibilities.

The management team must set expectations for actions staff should take in certain situations and then hold them accountable. This increases the level of risk awareness in your culture, allowing employees to identify key risk indicators and consider all possible trade-offs.

4 HOLISTIC, ENTERPRISE-WIDE DESIGN

ERM is a set of principles that builds a standard framework, compiled by COSO, to help organizations design and implement procedures with a holistic view of strategy, risk, and performance. The framework has five components:

- *Governance & culture*
- *Strategy & objective setting*
- *Performance*
- *Review & revision*
- *Information, communication, & reporting*

We'll talk further in section three about how these five components shape, and connect, strategy, risk, and performance.

EXAMPLE 1

A financial services client identifies the lack of an updated business continuity and disaster recovery plan (BCP and DRP) through enterprise risk management discussions. This risk is identified as a low-likelihood, but high-impact risk. The ERM process brings the risk to the attention of key stakeholders, who then make updating the company's BCP and DRP a key priority in the annual plan. By implementing their updated BCP and DRP, the client is able to make informed business decisions in response to natural disasters, global pandemics, and other unexpected events, and continue uninterrupted business operations.

COSO Enterprise Risk Management — Integrating with Strategy and Performance: Compendium of Examples

Enterprise risk categories

OPERATIONAL RISKS

Risks that directly affect the day-to-day operations of a business. These risks are measured by the severity of the interruption to daily operations. The longer the interruption lasts, the more severe the impact is to the organization.

» ***Examples:*** *legal risk, environmental risk, network infrastructure, or physical security risk*

FINANCIAL RISKS

Risks that impact an entity's financial position or performance. Some risks can cause a much greater financial loss to the organization than others.

» ***Examples:*** *currency risk, fraud risk, economic downturn, or high interest rate risk*

STRATEGIC RISKS

The risk of poor decision-making causing a strategy to be unsuccessful and therefore causing a loss to the business. Strategic success results from achieving business objectives. Failing to meet key business objectives can negatively impact the strategy.

» ***Examples:*** *liability risk, innovation risk, competitors, or branding risk*

COMPLIANCE RISKS

Legal and regulatory risks that arise from changes in the organization's standing with applicable governing bodies. Risk events in this category may directly and materially impact operations, financial standing, and organizational strategy.

» ***Examples:*** *labor and employment law, Sarbanes-Oxley (SOX) requirements, Health Insurance Portability and Accountability Act (HIPAA), European Union General Data Protection Regulation (GDPR)*

By examining all possibilities with respect to a particular strategy, doors open to discovering new opportunities for the entity. When ERM is integrated with strategy-setting and performance practices, an organization improves its ability to identify and pursue opportunities that create value, while also taking into account its risk appetite and business objectives.

Critical success factors of ERM

ERM success is driven by four key factors:

1 OWNERSHIP

Risk owners are assigned and understand their responsibility for management, oversight, and assurance.

2 ASSURANCE

Stakeholders are assured risk is being managed within the organization's risk tolerance and receive information about the quality and type of control in place.

3 OVERSIGHT

Critical risks facing the organization are identified, managed, and reported with a level and frequency that supports the organization's risk tolerance. This is a key component of a risk-conscious culture.

4 VISIBILITY

Management has clear visibility of the risk universe through dashboards that show and monitor controls and residual risk. Management also has an actionable playbook ready to execute.

Implementing these success factors support the integration of ERM practices throughout the organization. This results in improved decision-making in governance, strategy, objective-setting, and day-to-day operations, and will lead to enhanced performance through the creation, preservation, and realization of value.

ERM and its impact on organizational culture and capabilities

Applying ERM can empower your organization to optimize two key areas: culture and capabilities, and a successful ERM framework starts with your organizational mission and vision. While most tend to think of ERM as the core discipline and vehicle for risk prevention, effective ERM can also identify favorable risk-taking situations that present potential opportunities for the organization — depending on your organization's risk appetite. But no singular, uniformly applied risk appetite exists for all entities. Rather, management and the board of directors develop and refine the organization's risk appetite, both quantitatively and qualitatively, using available information and an understanding of the risks and rewards involved.

OVERALL RISK APPETITE DRIVES AND DETERMINES:

- ✓ How the organization identifies risks.
- ✓ Types of acceptable risk.
- ✓ How risks are managed.

These three factors influence how an organization positions itself on the culture spectrum, which ranges from risk averse to risk aggressive. The closer an organization is to the risk-aggressive end of the spectrum, the greater its propensity for and acceptance of certain risks in order to achieve strategy and business objectives. On the other hand, the closer an organization is to the risk-averse end of the spectrum, the lower the organizational risk appetite.

The guiding principles of the ERM framework emphasize the importance of integrating ERM into the culture, capabilities, and practices of an entity. This ultimately results in better decision-making and further integrates ERM into all aspects of the organization.

ERM can also identify favorable risk-taking situations that present potential opportunities for the organization.

Culture

Every organization wants its culture to exemplify a specific message or behavior. With regards to risk management, organizations should strive for risk awareness to be an evident — and emphasized — aspect of their culture.

The tone at the top of an entity cascades to all staff. If management and the board can develop risk awareness from above, it becomes an organizational social norm and is more likely to be followed at the individual level. Risks will be anticipated earlier and more clearly, minimizing adverse impacts on performance.

This takes significant commitment. Organizations must take risk into consideration with any and all decisions made, no matter the magnitude. Staff should be encouraged to think critically about risk management and voice concerns they have about decisions and policies without fear of punishment or backlash.

When ERM is fully integrated with an entity's business activities, organic risk-oriented decision-making becomes embedded in its culture. A risk-conscious culture considers how risks can impact all areas of the organization, allowing for improved collaboration among risk owners. Evaluation decisions become more complete, and risk-response decision-making is more informed.

When ERM is fully integrated with an entity's business activities, organic risk-oriented decision-making becomes embedded in its culture.

Capabilities

ERM gives management full visibility of whether the organization is at risk of not meeting business objectives. The capability of an organization to successfully meet business objectives relies on the entity's people, processes, and technology. To accomplish this, management must make readily available the resources and tools needed to fulfill ERM responsibilities. Resources include the technology to support the process as well as the skilled individuals who can see the process through.

PEOPLE

When all managers and executives take part in ERM discussions, communication about risk management is reinforced within the entity's culture. By following leadership and examples set by management, staff begin to feel comfortable speaking up about concerns and ideas they might have about risk management and risk engagement activities.

PROCESS

To successfully integrate the ERM framework into your operations, your organization must have an established reporting structure, otherwise it's difficult to manage and monitor risks. Frequent and effective communication is key to ensure correct information is passed between management and staff.

TECHNOLOGY

Strategic goals and outcomes should be measurable and achievable. Using technology to create dashboards or metrics reports, for example, allows an organization to gain visibility into their ERM framework risks. These tools help track and monitor that an organization is fulfilling its ERM responsibilities and, in doing so, improving performance monitoring and effectiveness.

EXAMPLE 2

A large real estate organization tries to implement an ERM framework, but management realizes the entity doesn't have enough staff resources for monitoring — no one has the availability to ensure ERM responsibilities are being fulfilled. Because risk monitoring and goal tracking aren't feasible, the organization cannot implement the framework.

COSO Enterprise Risk Management — Integrating with Strategy and Performance: Compendium of Examples

Building the ERM framework

This section will walk you through the five components of the ERM framework: governance and culture, strategy and objective-setting, performance, review and revision, and information, communication, and reporting.

GOVERNANCE AND CULTURE

The board of directors establishes the tone and culture at the top of the organization. Because culture both influences and is influenced by decision-making, the importance of ERM should be initially communicated during strategy-setting, and continuously reinforced through structured decision-making for key organizational initiatives. This encourages all members of the organization to think critically about risk management, ultimately embedding ERM into the organization's mission, vision, and values.

STRATEGY AND OBJECTIVE-SETTING

ERM is incorporated into the strategy-setting process by identifying the risk profile associated with the strategy under consideration. The strategy's business objectives drive its success since it ensures all team members have the same goals.

EXAMPLE 3

An insurance company only has a few large clients generating all of its revenue. They decide to begin targeting smaller insurance groups to mitigate the risk of losing one, or multiple, large clients. Setting this objective helped the company avert a potential revenue loss associated with losing large accounts.

COSO Enterprise Risk Management — Integrating with Strategy and Performance: Compendium of Examples

PERFORMANCE

The ERM process helps an organization determine what risks may prevent the success of a given strategy as well as its responses to said risks. This portfolio view gives an idea of the total amount of risk associated with the strategy, helping organizations understand the relationship between risk and performance — ultimately enhancing performance overall. It allows management to consider the type, severity, and likelihood of risk events, and how those events may affect performance.

REVIEW AND REVISION

To evaluate how ERM practices affect an organization, management must review the associated performance. An entity can have mitigation practices in place, but they won't be effective if appropriate personnel don't evaluate or audit those practices to ensure the risk is truly mitigated. Regular review of risk management practices allows risk owners to make necessary adjustments to improve the process further.

INFORMATION, COMMUNICATION, AND REPORTING

Effective communication between management and stakeholders is critical to achieve ERM objectives and to capitalize on business opportunities. This starts by ensuring that risk management roles and responsibilities are clearly defined and understood. As such, management must communicate strategic and business objectives, expectations, desired behaviors, performance targets, and key risk indicators clearly so that all personnel at all levels understand their individual roles.

EXAMPLE 4

To mitigate physical security risk, a company requires staff to have badges that allow them access to the building. To ensure this process is effective, the organization periodically tests whether staff can access the building without a badge.

EXAMPLE 5

Through the ERM process, an organization develops a risk playbook that conveys the implemented plan for every risk that could occur. This documented action plan states how the entity will respond to each risk as well as who is responsible for responding. Documenting and communicating this information between the risk/control owners and upper management increases the likelihood the plan is executed properly.

COSO Enterprise Risk Management — Integrating with Strategy and Performance: Compendium of Examples

How successful organizations put ERM into practice

Through the ERM process, organizations discover and understand inherent risks to their entity that are associated with a specific strategy. By identifying potential situations before they happen, an organization can proactively manage those risks to limit the impact on their operations. Consider these practical risk management guidelines:

1. *Assess and prioritize risks*
2. *Implement a plan*
3. *Put risk management practices in place*
4. *Clearly communicate expectations*

By identifying potential situations before they happen, an organization can proactively manage those risks to limit the impact on their operations.

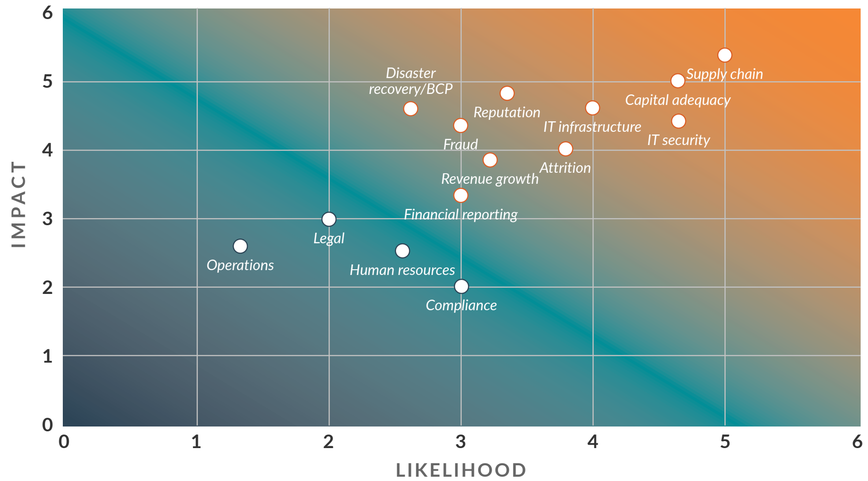
1 Assess and prioritize risks

Discussing potential risk events allows the entity to examine all aspects of strategy and performance. These discussions are a critical step and the single most important factor in determining the contours of the organization's risk management framework. Discussion also serves as the basis for assigning priority to identified risks and for resource deployment.

DEPICTING RISK PRIORITY WITH A RISK HEAT MAP

The heat map below depicts the risk priority among all risks in the organization's risk universe on a two-dimensional scale. Risks that represent the highest impact and likelihood, such as those with a profound and immediate impact on strategic business objectives, appear in the upper-right area of the map. On the contrary, risks representing the lowest impact and likelihood, such as those with a limited to moderate effect on the success of the organization, appear in the lower left area of the map.

HEAT MAP



The assessment and prioritization of risks includes:

INTERVIEWS TO IDENTIFY THE RISK UNIVERSE
- *Interviews with key personnel*
- *Creation of criteria for risk universe and impact and likelihood of risk*

INHERENT RISK ANALYSIS
- *Inherent risk analysis*
- *Ranking of inherent risks*
- *Clear understanding of:*
  - » *Risk assessment process*
  - » *Risk universe*
  - » *Impact and likelihood criteria*

MITIGATION STRATEGY ANALYSIS
- *Inventory of mitigating activities*
- *Delegation of ownership*

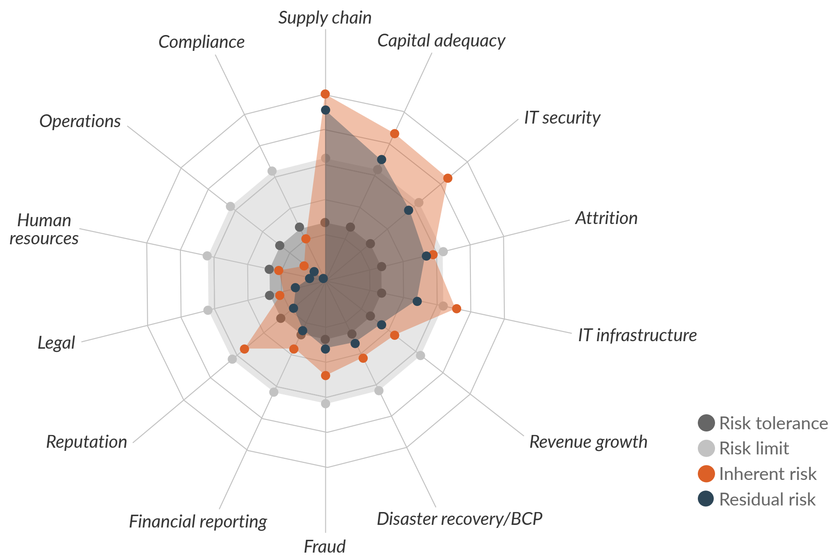
REPORT GENERATION
- *Results and themes*
- *Summary of risk treatment plans*
- *Radar chart, bullet chart, heat maps*

TEST RISK TREATMENT PLANS
- *Ensure implementation of items outside of risk tolerance*

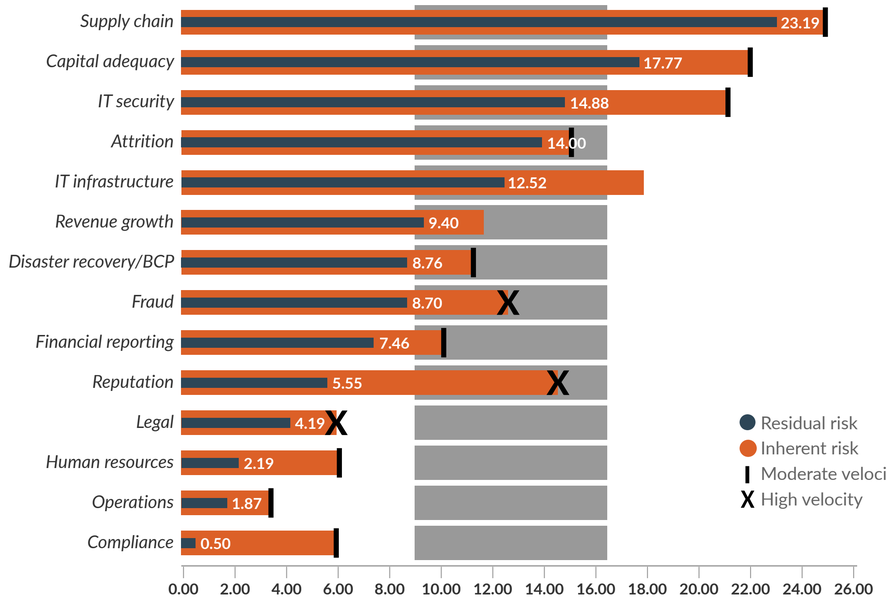
DEPICTING THE RISK UNIVERSE WITH RISK DASHBOARDS

The diagrams below depict an organization's enterprise risk universe. These dashboards represent the organization's risk tolerance level versus high-risk events falling outside the tolerance level that need to be mitigated.

RESIDUAL RISK RADAR CHART



RESIDUAL RISK BULLET CHART



2 Implement a plan

While some of the ERM process is geared toward proactively managing situations that your organization may experience, simply recognizing inherent risks won't change the outcome of those situations. The goal is to implement a risk management playbook — a plan, or adjustment to an existing plan, that limits the negative impacts on your organization by clearly communicating the roles and responsibilities associated with risk management activities. The risk management playbook incorporates key facets of each risk treatment plan:

- *Risk owner*
- *Identified internal controls, risk management activities, & corresponding owners*
- *Specific scenario-based action plans*
- *Communication protocols*
- *Activity timelines*

SAMPLE RISK PLAYBOOK

COMPETITOR RISK

Risk description

Competitors or new entrants to the market take actions to establish and sustain competitive advantage over the company or even threaten its ability to survive.

Risk owner: John Smith

Control owner: Mary Smith

Playbook summary:

This playbook focuses on an action plan for threats to sustaining/improving our competitive position in the market.

ACTION PLAN(S)

RISK SCENARIO IDENTIFIED BY SALES/UNDERWRITING

- *An incident or movement occurs in the market causing a major shift in the competitive position of the company, thus negatively impacting our ability to grow or retain business, created by one or more carriers.*
- *Bundling or embedding of health benefits becomes the norm.*

SALES/UNDERWRITING DEPARTMENT SUBJECTIVE ASSESSMENT

- *Nature and scope of the issue (i.e., product-based, specific rate segment, risk and/or ASO)*
- *Assess urgency*
- *Impact directly affecting new business, renewals, or both and at what level*

SALES DEPARMENT ACTIONS

Monitor situation

- *Work with sales and underwriting to determine if isolated situation with one carrier or emerging trend*
- *Provide updates to ERM team and/or executive team as needed*
- *Determine when board notification is necessary*

Monitor and proactively prepare

- *Prepare internal talking points and plan of action*
- *Notify internal departments as needed*
- *Provide updates to ERM team and/or executive team as needed*
- *Determine when board notification is necessary*

Activate response/communications protocol

- *Determine corrective action plan to mitigate risk based on specific market segment issue with rates*
- *Determine necessary internal and any external communication messages and the proper channels*
- *Prepare and distribute internal resources for Sales team if needed*
- *Draft board notice, including communications and resources*
- *Prepare and distribute communications*
- *Prepare and distribute external FAQs*

Responsible internal personnel:

John Smith *Mary Smith*

Third parties involved and contact information: N/A

3 Put risk management practices in place

The ERM framework delivers the most value through the practices management puts in place to actively manage the risks to their organization. A risk management system gives the organization an effective way to learn, monitor, and improve performance.

REMEMBER:

At its core, ERM is a process intended to support management's identification of potential events that represent risks to the achievement of strategic objectives and opportunities for organizational growth. This process requires that risk identification and assessment activities are addressed with internal controls, monitoring responsibilities, and strong organizational governance.

4 Clearly communicate expectations

Clearly communicating risk management responsibilities to each team member is critical to set expectations and hold individuals accountable when necessary. This approach doesn't place blame on an individual, but rather encourages a greater understanding of risk management and continual improvement. During strategy-setting sessions, ERM allows management to consider inherent risks to the organization within the context of specific organizational initiatives. Building from there, the discussion must include how the organization can limit the impact of each risk, and how it's going to respond if the risk becomes a reality.

EXAMPLE 6

An organization's leadership is lacking when it comes to creating a risk-conscious culture. When employees attempt to voice concerns about risk management, they're ignored. Key risk and control owners aren't being held accountable for fulfilling ERM responsibilities.

A customer of the company overhears a staff member saying rude and degrading things about him. The customer goes to the media and voices concerns about the organization's management and customer service capabilities. This reputation risk sheds light on the organization's inability to mitigate potential risks to its operations.

In response, management and the board make it a priority to imbed enterprise risk management into their organization's culture. Key personnel are given the responsibility to ensure staff are thinking critically about risk management and encouraged to speak up about risk-related matters. The organization also puts training modules in place to set a formal expectation of how management wants staff to respond to risk-related events. Monetary incentives are offered to further promote this desired behavior.

To track and monitor staff performance, human resources documents training records and follows up with staff when an individual doesn't complete the modules. This, too, improves accountability.

COSO Enterprise Risk Management — Integrating with Strategy and Performance: Compendium of Examples

BACK | NEXT

In conclusion: Risk and resilience

As you successfully manage individual risks, ERM is further integrated into your organization — culturally, strategically, operationally. An organization's response to both identified and unanticipated risks reflects its capability to make appropriate decisions that align with the scope and speed of the risk at hand. The results can then be assessed and used to improve ERM practices in the future, which enhances performance.

As you successfully manage individual risks, ERM is further integrated into your organization — culturally, strategically, operationally.

ERM isn't simply a "check-the-box" exercise; significant value emerges through the many discussions to be had about how the organization can:

1. *Prevent the likelihood of an event occurring.*
2. *Manage the impact to the organization when an event does occur.*
3. *Identify opportunities for risk-taking rewards.*

The value of an organization is influenced heavily by the quality of its collective decisions. Risk awareness and effective risk management are crucial factors for sound decision-making and, as a result, driving value. ERM supports timely decision-making about how best to respond to events that present an operational, financial, or strategic challenge to an organization. Taking all aspects of the business into account holistically through the ERM framework improves the likelihood of favorable outcomes and minimizes the possibility of negative impacts.

All organizations today, regardless of industry or structure, face significant, constantly changing risks that are gaining in speed and impact. An ERM framework helps organizations better anticipate, navigate, and minimize the negative effects of these threats to improve resilience. The bottom line is, when done well, an ERM framework enhances performance and helps you create, preserve, and realize value. Is your ERM framework delivering?

Resources:

Contact us

Troy Snyder, partner
troy.snyder@plantemoran.com
248-223-3273

Jack Kristan, partner
jack.kristan@plantemoran.com
248-223-3605

Matthew Bohdan, principal
matthew.bohdan@plantemoran.com
248-223-3619

MC GH01.072220