Deloitte.

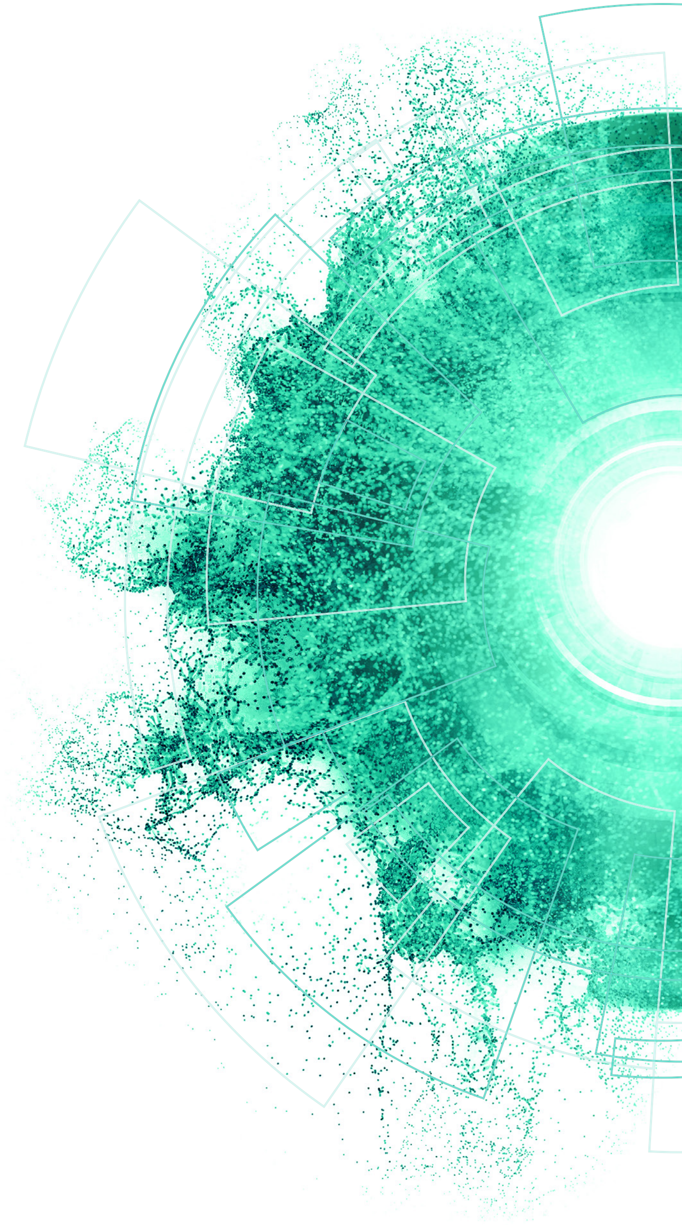
Creating a Risk Intelligent Enterprise: Risk governance

Risk governance: Overseeing risk and risk management

Robust risk governance drives a consistent and coordinated approach to risk across the organization and gives leaders a clear line of sight into risks and opportunities. Yet too many organizations still lack a well-defined system of risk governance or have established risk governance only in certain areas of the business rather than at the enterprise level. Many take siloed approaches to risk, which tend to focus on individual, site-specific threats. Such outdated methods serve the enterprise poorly in our environment of ongoing disruption. They can also leave management blind not only to certain risks but also to the opportunities that risks present.

The Risk Intelligent Enterprise aims to align risk management with organizational strategy and to promote an integrated approach to risk management and assurance.[1] An enterprise-level approach to risk governance enables the Risk Intelligent Enterprise. An effective enterprise risk governance structure supports the Risk Intelligent Enterprise in maturing its capabilities while avoiding the common pitfall of capabilities becoming siloed.

Enterprise-level risk governance underpins the Risk Intelligent Enterprise while enabling capabilities such as portfolio optimization, risk sensing, and scenario planning and war-gaming (also covered in this series on *Creating a Risk Intelligent Enterprise*). In other words, the Risk Intelligent Enterprise is enabled by enterprise-level risk governance, which also positions the enterprise to optimize returns from additional risk-related capabilities.



[1] "Reimagining the Risk Intelligent Enterprise," Deloitte Development LLC, 2018.

Three key questions

To govern risk effectively, management and the board need a practical approach to risk governance and the operational discipline to implement that approach at the enterprise level. This raises three questions that management, the board, and others concerned with risk in the organization should ask:

1. **Do we currently exercise risk governance at the enterprise level?**

2. **How can we better align risk governance and risk management across the enterprise?**

3. **How can we drive risk management into our day-to-day business practices?**

Deloitte's approach to risk governance assists management in answering these questions.

First, even in today's disruptive environment many companies continue to exercise risk oversight in siloed ways that limit management's and the board's view of risk. Risk intelligent risk governance recognizes the need for enterprise-wide views of and approaches to risk, and works to establish those views and approaches.

Second, risk intelligent risk governance aligns the organization's risk strategy with its business strategy. This enables management to view risk not just from the traditional standpoint of loss prevention but also through a value-creation lens. This expands management's view to include the opportunities that risks present rather than only the potential for loss, and promotes alignment of risk governance and risk management.

Third, if the organization is to address risk effectively, risk management must be integrated into day-to-day business practices. This calls for establishing protocols for identifying, monitoring, and communicating about risk at the operating level across the enterprise and then putting the right risk-related information in the hands of the right people at the right time.

Organizations need integrated views of risk, formal risk governance policies, and coordinated responses to risk events, as well as tools that enable risk management. It is the risk management function's responsibility to develop these enabling tools and to facilitate coordination among siloed areas; however, it is the senior leaders' duty to foster adoption of those views, policies, and responses. Without strong tone-at-the-top, many organizations fail to achieve their risk management goals.

How does it work?

Every organization must develop its own approach to the risks of its business. Yet there are distinct steps that senior leaders can take to establish sound risk governance, which stands apart from and oversees risk management.

IDENTIFY ALL RISKS AND DEVELOP AN ENTERPRISE-WIDE VIEW OF RISKS

Risk intelligent risk governance begins with identifying and assessing all risks to the organization. It then goes on to develop a common language of risk and an enterprise-wide view of risk. Rolling up all risks to the enterprise level enables management to understand the total exposure of the organization, within and across risk types, in all businesses and functions. This process aggregates risks and helps in identifying interrelationships among risks and ways in which risks may amplify one another. For example, operational risks can generate financial risks, which can generate reputational risks—and all of these risks must be recognized and addressed. This process also fosters cross-functional discussions about risks.

ASSIGN RISK-RELATED ROLES AND RESPONSIBILITIES

Virtually every job function has risks associated with it. The three lines of defense model of risk management and governance can be useful here. In this model, the first line of defense—the business—manages the risks because that is where the risks are located and where they can be managed most effectively. The second line—supporting functions such as compliance, legal, and risk management—helps the first line to define standards, adopt leading practices, connect business leaders across the organization, and develop relevant tools and mechanisms. The third line—internal audit—provides assurance that risks have been identified and management has addressed them. Clearly defined roles and responsibilities are essential to risk governance.

DEVELOP A RISK GOVERNANCE INFRASTRUCTURE

The risk governance infrastructure comprises policies, procedures, and practices of risk oversight as well as the tools that operationalize them. For example, risk governance depends on relevant, timely risk data so exposures can be monitored and controlled. That data must be communicated to the right people at the right time and in the right ways in order for them to make risk-informed decisions. Clearly defined risk appetite, risk profile, and risk tolerances enable management and first-line teams to understand risk exposures, communicate more clearly about them, and more effectively control them. In addition, the right risk culture—in which the organization's business strategy and risk strategy, and messaging, conversations, and incentives related to risk are all aligned—can be considered part of this infrastructure.

PROVIDE THE RIGHT RESOURCES

Organizations need the right people, processes, and technologies in place to implement and maintain the risk governance infrastructure. People need the requisite expertise and experience to manage the risks within their job functions. Processes for risk management should, to the extent possible, be integrated into operational processes rather than tacked on as check-the-box exercises. That calls for supporting technologies that enable people to identify, monitor, analyze, and manage risks. Policies and procedures cannot implement themselves. Senior leaders must provide the budget and other resources to enable the organization to implement them.

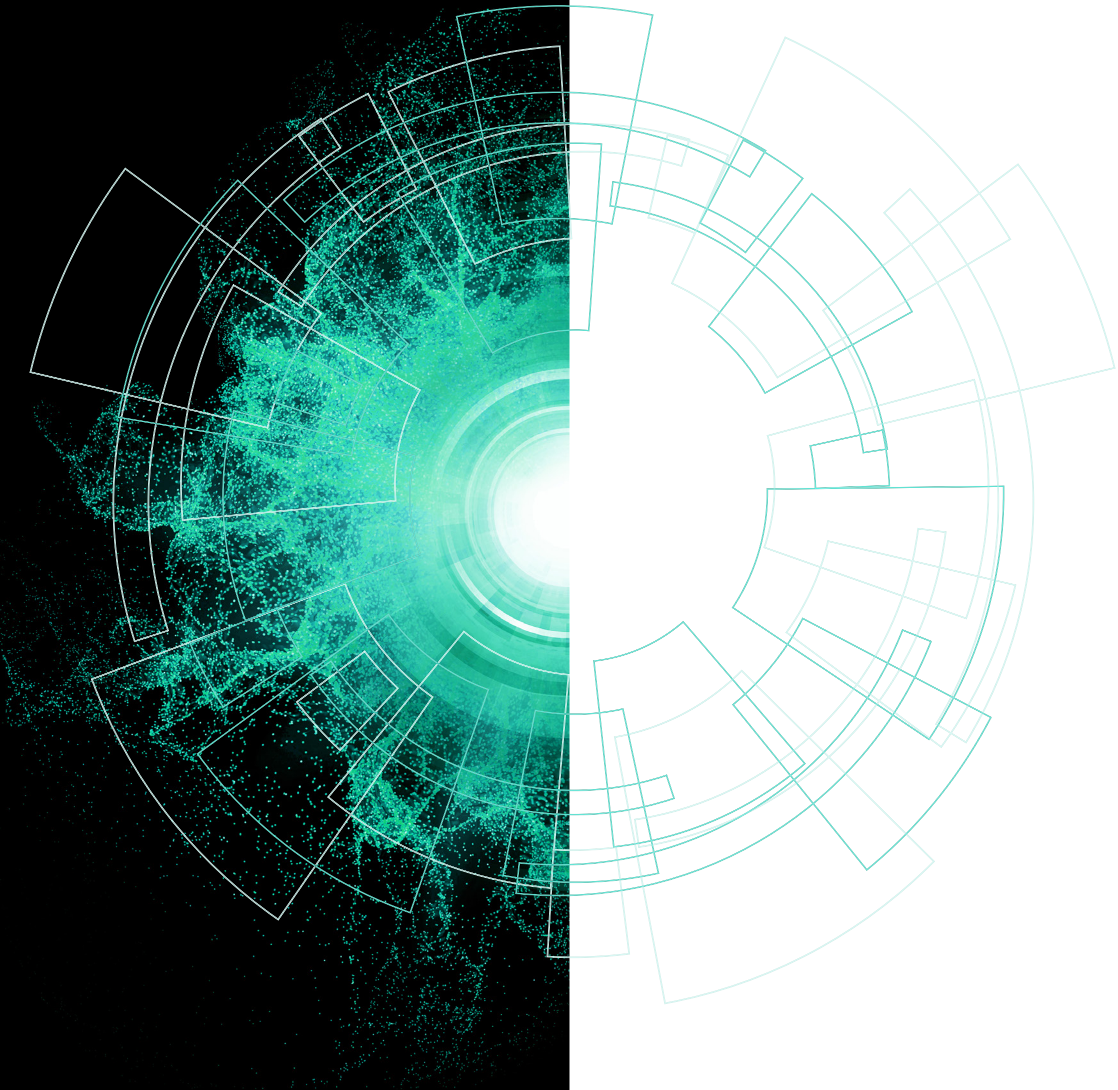
True risk governance occurs throughout the organization. While senior-level governance must ascertain that critical risks are managed and that the right decisions are made, the effort must cascade into the functions and lines of business. By the same token, the functions and lines of business need clarity as to when risk information needs to be escalated upward. Also, discussions and decisions around risk acceptance, mitigation, and escalation should occur as part of business discussions, so as to integrate risk into decision making and into the broader strategy and mission of the organization.

Getting it right

Sound risk governance ascertains that the organization is taking the right risks, in the right amount, for the right potential rewards while controlling losses. It also helps management take minimal amounts of unrewarded risks, such as certain legal and compliance risks.

The trappings of risk governance should not be mistaken for the practice of risk governance. A risk committee, risk limits, and risk reports do not in themselves constitute risk governance. Risk governance must be built into the work of the organization. Similarly, training about relevant risks should be part of the orientation to every job function. In that way, risk management, as well as risk governance, becomes woven into the organizational culture.

While risk governance will always remain a work in progress for most organizations, that work stands among the most vital activities that senior leaders can undertake, particularly within a Risk Intelligent Enterprise.



Contacts

Please share this perspective with your teams and contact us when you're ready to start your Risk Intelligence journey.

Cynthia Vitters
Managing Director | Risk Intelligence
Deloitte & Touche LLP
cvitters@deloitte.com

Ryan Morgan
Senior Manager | Risk Intelligence
Deloitte & Touche LLP
rymorgan@deloitte.com

Deloitte.

This document contains general information only and Deloitte Risk and Financial Advisory is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte Risk and Financial Advisory shall not be responsible for any loss sustained by any person who relies on this document.

As used in this document, “Deloitte Risk and Financial Advisory” means Deloitte & Touche LLP, which provides audit and risk advisory services; Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.