Improve Your **Grip**

Boost performance | Be responsible | Build trust

A guide for senior executives and boards

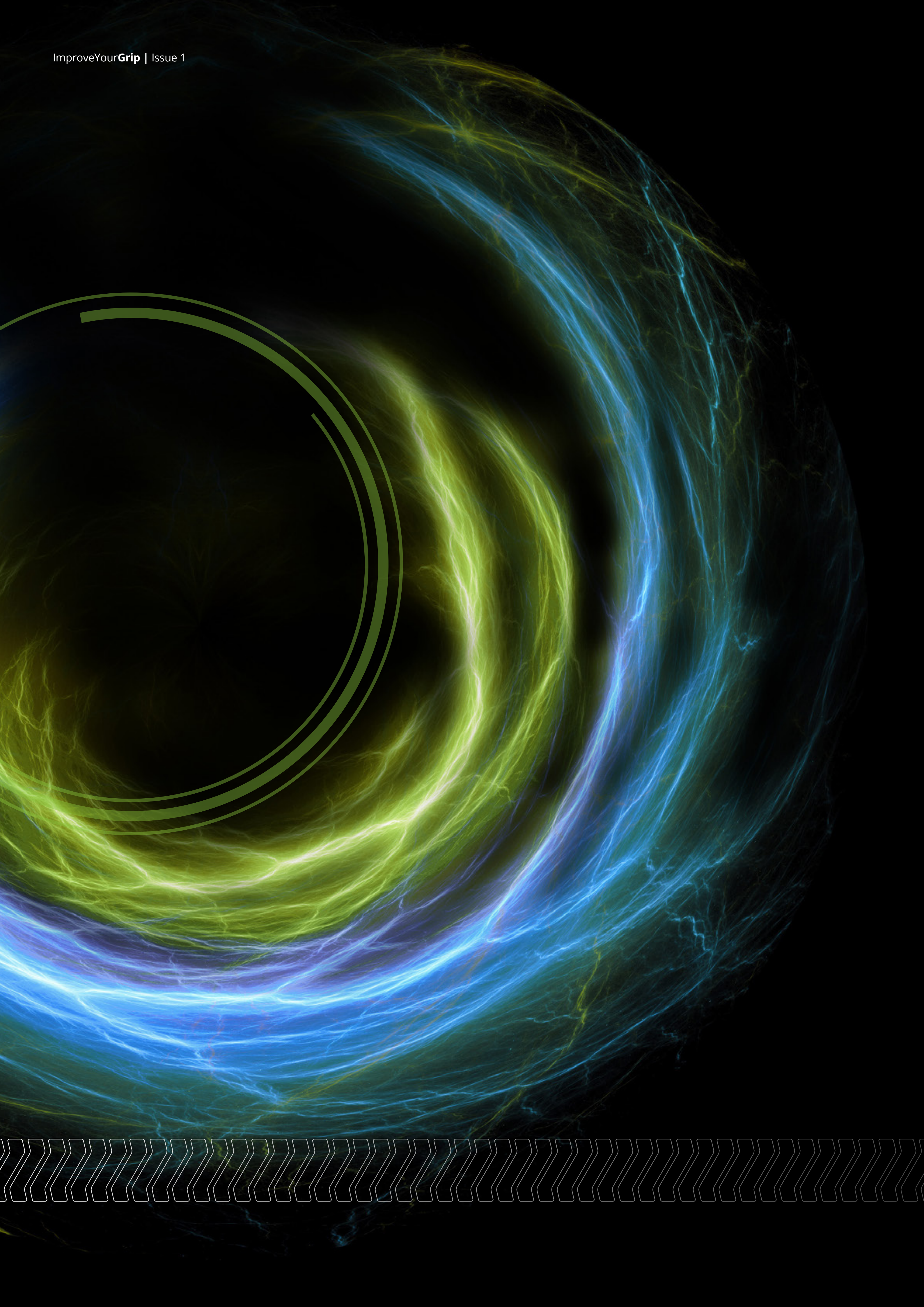
Issue 1 | Global

GET A GRIP
Improving your grip on risk governance often entails reviewing, refreshing, and revising risk-related practices.
Page 02

WHERE AND HOW TO START
Where and how you start to improve your grip on risk governance depends on how clear, practical, and robust your existing system of risk governance is.
Page 06

MAKING AN IMPACT THAT MATTERS *since 1845*

Deloitte.



Foreword

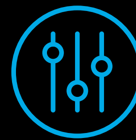
Recent years have severely tested risk governance and risk management capabilities at most organizations. Given the impacts of the Covid-19 pandemic and various cyberattacks, weather events, and political and social developments, it's a wonder that risk managers and the executive teams and boards who oversee them can keep pace with the challenges they face. In fact, some have not kept pace; others have been led to question their approaches to risk.

This is understandable. It is also a signal that risk-related practices of the past are often inadequate to challenges of the present, let alone the future. These challenges have been apparent for some time and include:

Ongoing digitalization of business models, processes, relationships, transactions, and currencies

Shifting social forces, ranging from environmentally conscious customers to activist investors

Widespread use of alliances, partnerships, and other elements of the extended enterprise



Economic uncertainty due to Covid-19 and its lingering impact

Evolving, often uncoordinated regulatory regimes within a globalized business environment

Downward pressure on budgets and headcounts amid mounting competitive pressures

Under these circumstances, senior executives and boards often need to improve their grip on risk governance, which sets the tone for and oversees risk management. This does not necessarily mean either tightening or loosening your grip on risk governance. It means establishing and maintaining optimal risk governance.

Optimal risk governance boosts performance by enabling risk-based decision making, which balances value creation and asset protection. It enables the executive team and board to fulfill their risk-related responsibilities by clarifying risks to the enterprise and obtaining assurance that those risks have been addressed. It builds trust by providing visibility into risks as well as assurance to stakeholders that they are being addressed.

This article aims to help senior executives and board members to consider their organization's risk governance, and the extent to which they need to enhance it to boost enterprise performance, better execute their risk-related responsibilities, and build trust among stakeholders.

GET A GRIP

Improving your grip on risk governance often entails reviewing, refreshing, and revising risk-related practices.

Our research and experience on client engagements indicates that this process is best undertaken with the goal of enabling risk-based decision–making while reinforcing the resilience of the enterprise in the face of risk events.

In general, sound risk governance results in: Risk management that includes but extends well beyond regulatory compliance. Risk-related practices that engage the business units and positions them to make better decisions. Greater visibility into risks, drivers of risks, and the effectiveness of risk-related practices. More effective deployment of not only risk management resources, but all resources. Higher levels of trust and comfort for customers, suppliers, investors, regulators, and other stakeholders. More confidence in senior executive decisions, both within the organization and among stakeholders.

If your business has been thriving, you may see it as immune to risk events and see little need to focus on risk governance. On the other hand, if your business must regain lost ground, you may believe you have higher priorities. In the former case, your organization may simply have been lucky; in the latter case, trying to regain lost ground without more robust risk governance may imperil the enterprise.

Whatever your current situation, risk events may well have exposed gaps, inadequacies, vulnerabilities, and inefficiencies in risk management and risk governance in your organization.

To be clear:

- Risk management encompasses risk identification and assessment, and monitoring, mitigating, reporting, and responding to risks. This occurs in the business, with functions such as cybersecurity, human resources, operational risk management, credit, and others providing support.
- Risk governance includes maintaining a strong culture, setting policies and procedures, monitoring risk profile, appetite, and tolerances, and providing assurance and oversight of risk management.

Sound risk governance—as opposed to "performative" risk governance (see sidebar)—enables executives to make better decisions given those uncertainties, and to explain those decisions if called upon to do so.

With the board's oversight and approval the senior executive team manages and governs risk, with the board ultimately responsible—and accountable—for governing risk on behalf of the shareholders and other stakeholders. Risk governance is linked, or should be linked, to business strategy. Executive teams constantly make decisions in light of uncertainties.

Question your current approach

Rather than review the goals of risk governance, let's turn them into questions for you to consider:

- Has your executive team and board developed an integrated, enterprise-wide view of risk? Do you consider that view when making decisions and allocating resources?
- Are you comfortable that your executive team and board truly understand the full range of risks that accompany strategic decisions and initiatives?
- Does your executive team set—and does the board approve—a risk appetite statement? Is risk appetite broken down into specific risk tolerances that managers and employees can use?
- Have you automated regulatory (and internal) compliance to the greatest extent possible?
- Have you taken full advantage of risk scanning, sensing, and reporting technologies? Do you link risk monitoring capabilities with clear issue escalation and risk remediation procedures?
- Do senior leaders participate in scenario development and risk response exercises? Does management use dry-runs to build "muscle memory" into organizational responses?
- Do you feel you have adequately identified risks beyond those well-known in your industry and organization, including economic, environmental, social, political, and reputational risks? Do you monitor stakeholder sentiment? Do you identify and track emerging risks?
- Have you fostered a culture of informed risk taking with sufficient transparency and accountability? Is your approach to risk management primarily proactive rather than reactive?
- Have you aligned your risk strategy with your business strategy? Have you aligned hiring practices, incentives, rewards, and other behavioral levers with your risk and business strategies?

A successful review and revision of risk governance will position your executive team and board to answer "Yes!" to each of these questions.

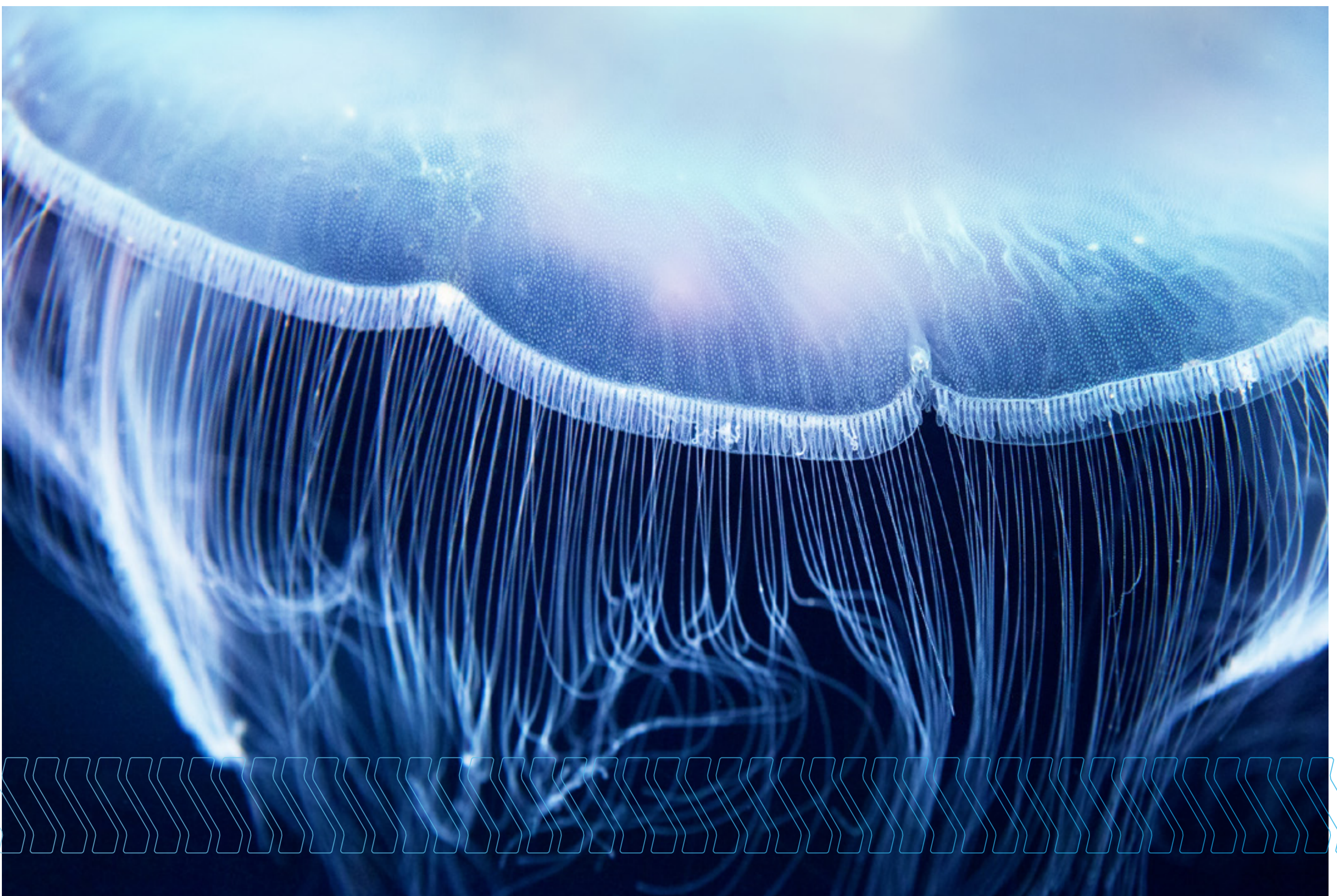
Avoid performative risk governance

In some organizations, risk governance is undertaken in a performative manner. Risks are identified, tracked, reported, and acted upon in habitual ways, and these tasks are seen as routine chores rather than vital activities.

Organizations engaged in performative risk governance tend to:

- **Confuse risk management with regulatory compliance:** Regulators focus on known risks and on their own needs, not on unknown risks and the organization's needs. Compliance should be automated to the extent possible, so people can focus on important emerging risks.
- **Aim mainly to minimize or avoid risk:** Risk taking is essential to value creation, and leaders who focus primarily on risk avoidance can be out-maneuvered by more aggressive competitors. Informed risk taking for value creation can generate superior results.
- **Manage risks in silos, through patchwork solutions:** Evolving risks call for new solutions, but adopting new solutions can lead to lack of coordination. A coordinated—and integrated—approach results in lower costs, greater transparency, and reduced risk.
- **Underinvest in risk management:** Mistaking risk management for compliance or a side-issue leads executives to underinvest in the people, processes, and technologies needed to address risk. Yet those are the resources needed to prosper in today's business environment.
- **Make risk governance difficult:** Lack of a coordinated, enterprise-wide approach to risk makes risk management and risk governance close to impossible. An integrated approach enables better decisions and results as well as more effective and efficient risk governance.

These mistakes can put an enterprise in a defensive crouch, when it should be playing offense and capitalizing on opportunities. Any one of these mistakes may indicate that your executive team or board is settling for performative risk management, and that you need a better grip on risk governance.



WHERE AND HOW TO START

Where and how you start to improve your grip on risk governance depends on how clear, practical, and robust your existing system of risk governance is. One good place to start making it clearer, more practical, and more robust would be to consider your existing governance framework. To assist you in this process, we provide our governance wheel.

Integrated assurance
Strategy and operating model
Risk management
Accountability and responsibility
Management information
Policies, procedures and controls
People alignment
Purpose, Leadership and Culture
Data & Intelligence
Communication
Technology
Training
Governing bodies
Governing bodies

Deloitte's Governance Wheel

The governance wheel summarizes the elements of corporate governance and the levers that the board and management can use to implement governance. Briefly, the components of the governance wheel include:

Strategy and operating model: Management sets the business strategy and develops the operating model with the board's input, approval, and oversight.

Accountability and responsibility: Management is accountable to the board and the board is responsible for governance of the organization and oversight of management's performance.

Policies, procedures, and controls: Policies, procedures, and controls translate the strategy and operating model—and accountabilities and responsibilities—to activities that people can perform as part of their jobs.

People alignment: Policies, procedures, and controls are most effectively implemented by people who are aligned with the purpose, mission, and goals of the organization, under the leadership and guidance of management.

Management information: People need information on the processes and controls they are using as they do their jobs, just as management needs information on the operational and financial performance of the organization.

Risk management: Uncertainty and risk accompanies virtually every business decision and initiative; therefore, oversight of risk and risk management is essential to corporate governance.

Integrated assurance: Both management and the board need assurance that systems are delivering accurate information and controls are effective; integrated assurance provides an enterprise view of the accuracy and effectiveness of the organization's information systems and controls.

With regard to risk, the elements of Deloitte's Governance Wheel operate in the following ways:

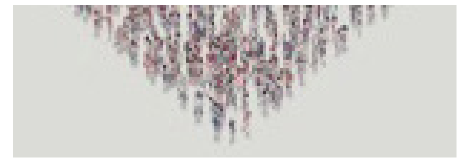
Strategy and operating model: Aligning the business strategy, operating model, and risk strategy ensures that the organization operates so that risk management is embedded in business operations. This flows through to development of a risk profile, risk appetite, and risk tolerances that align with the strategy and operating model. The result should be clarity around the organization's approach to risk, which enables risk-based decision making across the enterprise.

Accountability and responsibility: While senior executives and the board are ultimately accountable for risk, risk management occurs primarily in the business. To enable the business to manage risk effectively, leaders need to define clear risk-related roles, responsibilities, and accountabilities. This means identifying risks, risk management activities, and benchmarks at the level of the business, and properly delegating responsibility.

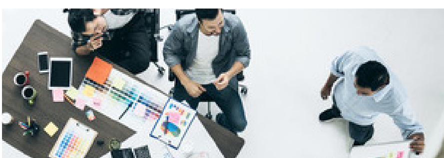
Policies, procedures, and controls: This component translates risk appetite and tolerances—and accountabilities and responsibilities—into things people can do to manage risk as they do their jobs. Leaders need to develop effective risk-related policies, procedures, and controls and promulgate them across the enterprise. This is not done by simply compiling manuals and checklists but by driving considerations of risk into day-to-day activities. Training, monitoring, and incentives, as well as actionable procedures and controls, make this happen.

People alignment: Particularly given the myriad risks in today's environment, the foregoing elements are not set-it-and-forget-it mechanisms. For example, management needs to lead people to internalize their operational and risk-related responsibilities in order to implement policies, procedures, and controls. This is no place for "management by memo." To align people with the business strategy, operating model, and risk strategy, leaders should set a clear example, provide consistent messaging, and establish congruent incentives.

Management information: The reliability, timeliness, and usefulness of management information, particularly risk data, affect everything from the competitiveness of the enterprise to its resilience in a crisis. Sound risk governance ensures that the organization leverages technology—and external as well as internal data—in its risk management. When applied to internal operations and the external environment, today's technologies can generate a true enterprise view of risk and support risk-based decision making.



Risk management: Proper risk governance calls for the board to obtain reasonable assurance that management has identified and addressed all key risks to the enterprise. This means ascertaining that management is aware of all key risks, has taken steps to mitigate them, and has planned responses to risk events ranging from minor incidents to full-scale crises. Risk management and risk governance aim to generate optimal results and returns, while balancing stakeholders' interests and protecting and enhancing shareholder value.



Integrated assurance: Integrated assurance helps efforts to rationalize assurance activities, achieve efficiencies, and direct resources to where they will do the most good. This is not to be confused with combined assurance, which often just rolls up existing reports or gets bogged down in assurance mapping exercises. Integrated assurance enhances visibility into risks and the effectiveness of risk management. It also creates a panoramic view of risks and risk management, which is essential to risk governance.

While the extent and emphasis will vary, the elements of this governance wheel will be found in most organizations. Breaking governance down into these seven components enables an executive team or board to consider the relative strength of each component. A framework like this can also help in identifying where a governance breakdown has occurred or could occur.

Like any wheel, our governance wheel must be properly balanced if it is to do its job. That means understanding where more or less attention, investment, and work is required, while recognizing that the executive team and the board must do the driving.

As you review your enterprise's risk governance, we suggest that you:

- Align your risk strategy with your business strategy in practical, as well as conceptual, ways.
- Identify the interplay among mission and values and the risk culture you are actually creating through leadership example, hiring practices, performance incentives, and other levers.
- Assess how you are using technology to enable processes, controls, and early warnings regarding risks across the enterprise—and to automate compliance and assurance.
- Develop a clear taxonomy of risks and translate risks that are inherently "technical" into business impacts. Also, encourage frontline workers to flag risks and challenge decisions.
- Consider your risk profile and where your organization could be taking more risk to drive greater reward. Also, look beyond the "risk du jour" in your industry to consider the black swan event that could undo your business model or empower competitors.
- Ask trusted stakeholders, such as key customers, suppliers, or investors about your risk posture; consider having an objective risk assessment conducted by a qualified external resource.

We trust that the foregoing will position your executive team and board to improve its grip on risk governance to enable your enterprise to thrive not only despite the risks in our environment, but because of those risks.

We also stand ready to assist you in any aspect of this process as you move forward.

GET IN TOUCH

DISCUSS THE REPORT AND LEARN MORE ABOUT OUR APPROACH

Authors

USA
Keri Calagna
US Risk & Financial Advisory Leader
+1 212 492 4461
kcalagna@deloitte.com

Canada
Prashant Masand
Canada Risk Advisory Leader
+1 416 643 8974
prmasand@deloitte.ca

Strategy, Brand and Reputation Leaders in Asia Pacific

Asia Pacific
Yusuke Nijo
Partner
+81 80 4341 5687
yusuke.nijo@tohmatsu.co.jp

Australia
Ian Blatchford
Partner
+61 2 9322 5735
iblatchford@deloitte.com.au

China
Jun RA Wu
Partner
+86 23 8817 7188
junwu@deloitte.com.cn

Japan
Hiroshi Miyazaki
Partner
+81 90 6501 1779
hiroshi.miyazaki@tohmatsu.co.jp

New Zealand
Aloysius Teh
Partner
+64 4 495 3934
ateh@deloitte.co.nz

New Zealand
Jane Fraser Jones
Partner
+64 4 470 3647
jfraserjones@deloitte.co.nz

Southeast Asia
David Chew
Partner
+65 6216 3271
dchew@deloitte.com

Southeast Asia
Yvonne Zhang
Director
+65 6932 5520
yvonnezhang@deloitte.com

Taiwan
Rick S. Wen
Partner
+886 2 2725 9988
rickswen@deloitte.com.tw

Taiwan
Mavis M. Hsu
Director
+886 2 2725 9988
mavismhsu@deloitte.com.tw

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities. DTTL (also referred to as “Deloitte Global”) and each of its member firms are legally separate and independent entities. DTTL does not provide services to clients.
Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 286,000 people make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms or their related entities (collectively, the “Deloitte network”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2021. Deloitte Global Risk Advisory

Designed by CoRe Creative Services. RITM751412