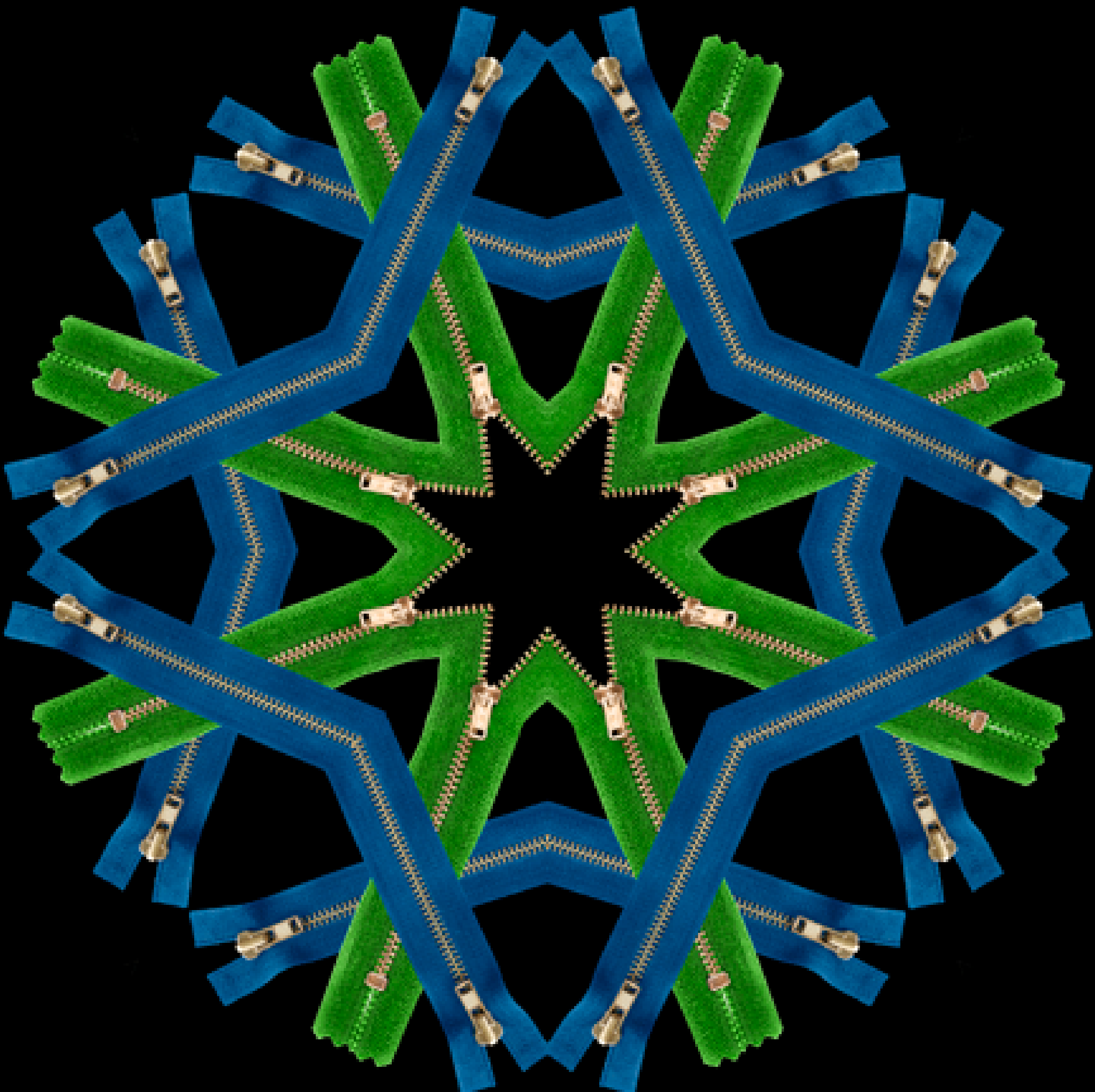
Deloitte.



Integrated risk assurance

Get a clearer understanding of the risks affecting business value

May 2018

Operational Risk

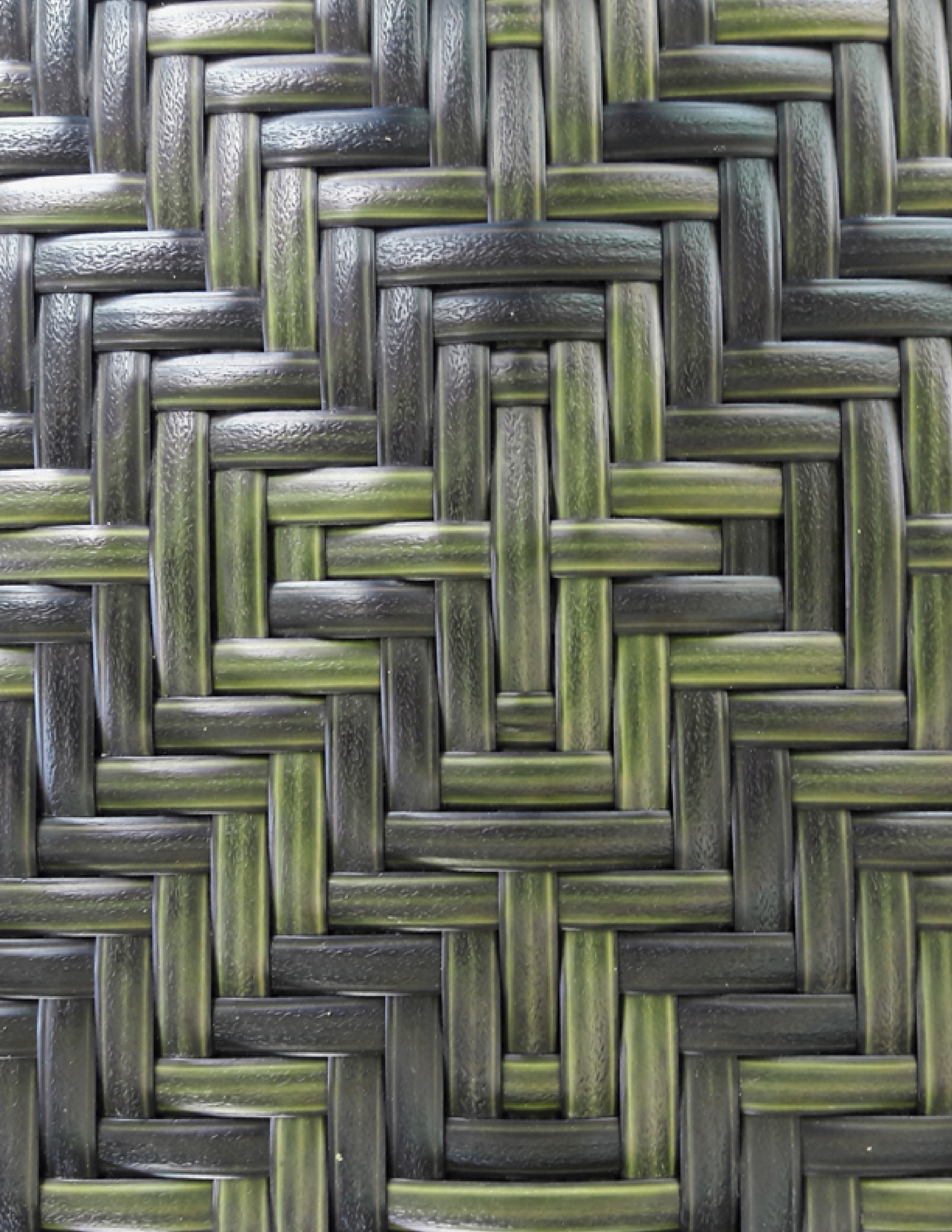
Contents

An efficient framework for seeing the whole risk picture

Over the past decade, as financial, operational, strategic, cyber, reputational, and other risks have proliferated, organizations have been working on effective responses. Boards have placed risk oversight at the top of their agendas. Senior executives have upgraded the risk management infrastructure. Businesses and IT functions have adopted tools and solutions. Compliance, risk management, and chief audit executives have enhanced their functions' capabilities.

Yet many management teams, audit committees, and boards still lack a clear, accurate, and comprehensive picture of the truly greatest risks to their organization and of the risk management programs that protect the organization. Ultimately, the purpose of risk frameworks and assurance activities is to strengthen an organization's controls to preserve shareholder value. From board directors to line managers, everyone occasionally loses sight of why these valuable governance mechanisms exist, relegating them to bureaucratic check-the-box exercises.

The main barriers to creating a comprehensive risk picture are neither technological nor financial but rather organizational, particularly when it comes to risk assurance. The traditional ways in which assurance activities and reporting are organized limit an organization's visibility into risks and into the effectiveness of its risk management, while creating unnecessary costs and exposures.



Defining the problem

Organizations have typically adopted new approaches to risk oversight and management in response to the most recent high-profile risk event in their organization or reported on the news, or in response to regulatory mandates. This has often resulted in risk reporting that's best characterized as narrowly focused and diffused, redundant and costly, intrusive to the businesses and functions, and, least pleasant of all, unrelated to the true drivers of enterprise value and performance.

If you're a senior executive or board member with risk-related responsibilities, consider these questions:

- Does the organization need to refocus on what really matters and clarify accountabilities for risk?
- Are assurance reports heavy on detail, but light on what those details mean?
- Is it difficult to reconcile the views you receive from various information sources for assurance?
- Do people in the business experience "assurance fatigue" due to multiple requests from various assurance functions?
- Does the term assurance need a better definition, along with a better definition of assurance responsibilities?

If you answered yes to any of these questions, it's time to consider integrated risk assurance.

But first, it's important to understand the two significant challenges facing current practices:

Issue 1

Too much information, not enough insight

Spurred by new regulatory mandates and the perceived need to mitigate all risks, there's been an explosion in assurance activities and reporting without an equivalent rise in insight on risks and risk management. Regulators and standard setters around the world have emphasized risk oversight and governance by boards and senior executives, and those overseers' roles in reviewing the effectiveness of risk management, but the data and details resulting from these stronger risk-management and governance efforts don't coalesce into a coherent picture on their own.

One response to these unconnected dots has been the development of the concept of combined assurance, which sought to take a fulsome view of all risk and controls in an organization. Combined assurance was first articulated in 2009 as a requirement for audit committees in South Africa's King III Corporate Governance Code.[1]

While the objective is conceptually sound, combined assurance efforts have often proven inadequate in providing what management needs. Most efforts tend either to roll up existing assurance reports or to bog down in mapping exercises to identify and rationalize every assurance activity in the organization.

Those flaws include burdensome, time-consuming activities geared mainly to assessing individual control, compliance, and risk management mechanisms and lack of attention to the big picture. These activities generate neither the insight into risks that boards and executive teams want nor the right levels of assurance on risk-management effectiveness.

In practice, every organization needs a bespoke, fit-for-purpose approach to integrating risk assurance. The purpose will vary with the organization, and its industry, regulatory environment, business strategy, specific risks, and available resources. The entity's level of risk assurance maturity will also help determine the proper approach.

Whatever the organizational needs are, a practical, enterprise-based approach to risk assurance must be rooted in the organization's specific drivers of value, the risks to those drivers, and ultimately in the needs of those relying on the assurance.

> "Good audit reports, but I can't see the forest for the trees"
>
> **- Board Member**

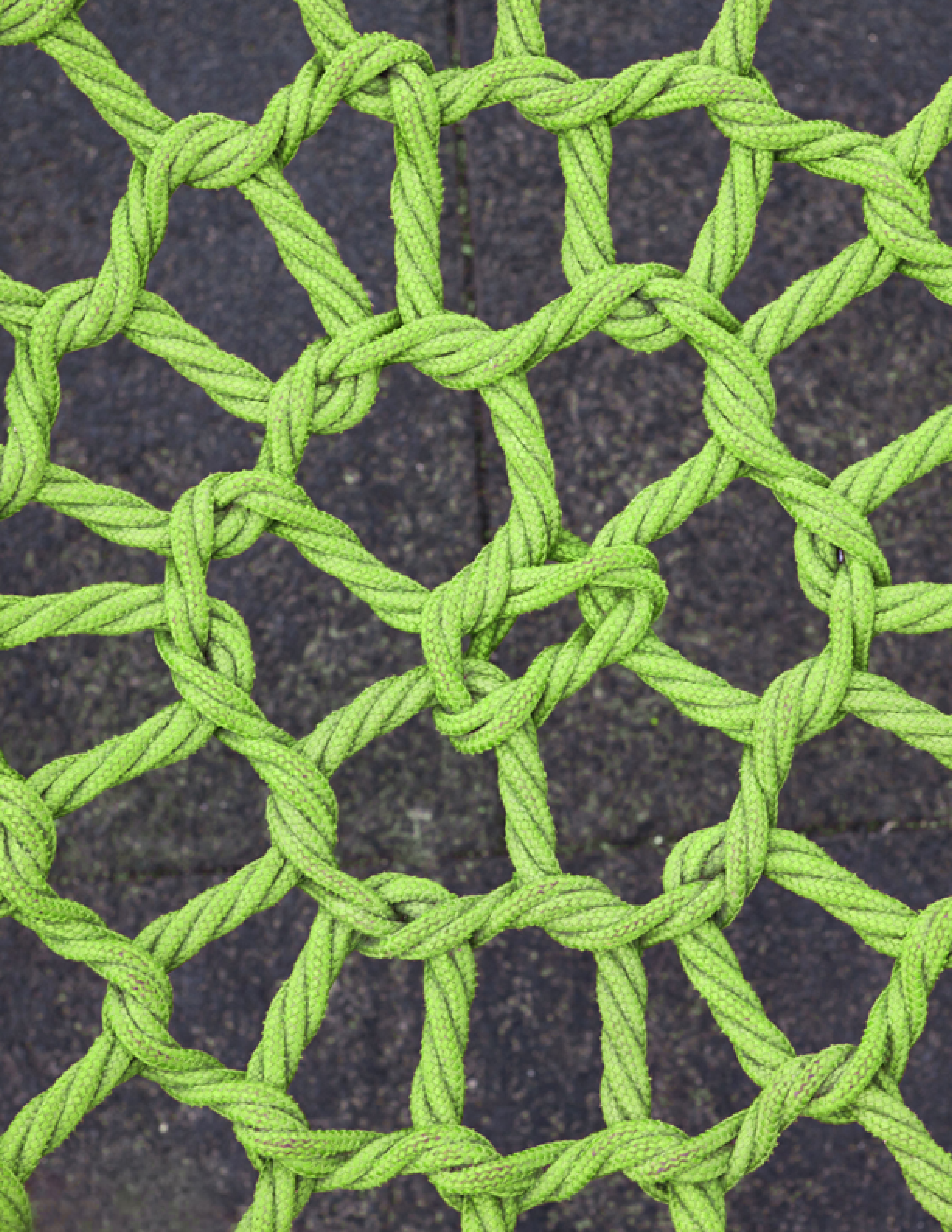
1. King IV: Bolder than ever, Deloitte South Africa, 2016 <https://www2.deloitte.com/content/dam/Deloitte/za/Documents/governance-risk-compliance/ZA_King_IV.pdf>

Issue 2
Risk serves multiple masters

Basic human instinct naturally drives us to manage risk in our personal lives. That instinct operates at an organizational level as well, but there the risks have various owners and overseers with different priorities and different risk-assurance needs. These owners and overseers include:

- **Board and audit committee members** who, as the ultimate overseers, require a clear view of risk; this view is often obscured by current methods of providing risk assurance
- **The chief executive officer,** who is responsible for implementing the strategies and achieving the performance goals that may be affected by risks and risk management
- **The chief operating officer,** who is directly accountable for decisions on operational performance and risk management
- **The chief financial officer,** who holds a major stake in the success of risk management as it affects financial performance and asset values
- **The chief risk officer,** who is responsible for supporting and overseeing risk management across the enterprise; this requires useful, high-quality risk assurance
- **The chief audit executive,** who aims to improve oversight of reporting, internal control, and audit processes, and must understand the organization's risks and risk management activities

Leaders must know what risks will affect their area of responsibility and who is ultimately accountable for managing those risks. However, a lack of coordination among risk assurance functions—and a lack of consensus on what matters most in risk and risk assurance—undermines efforts to develop an integrated view. More often than not, the challenge is that the complex risks overlap and accountability for them either sits with too many or no one at all.



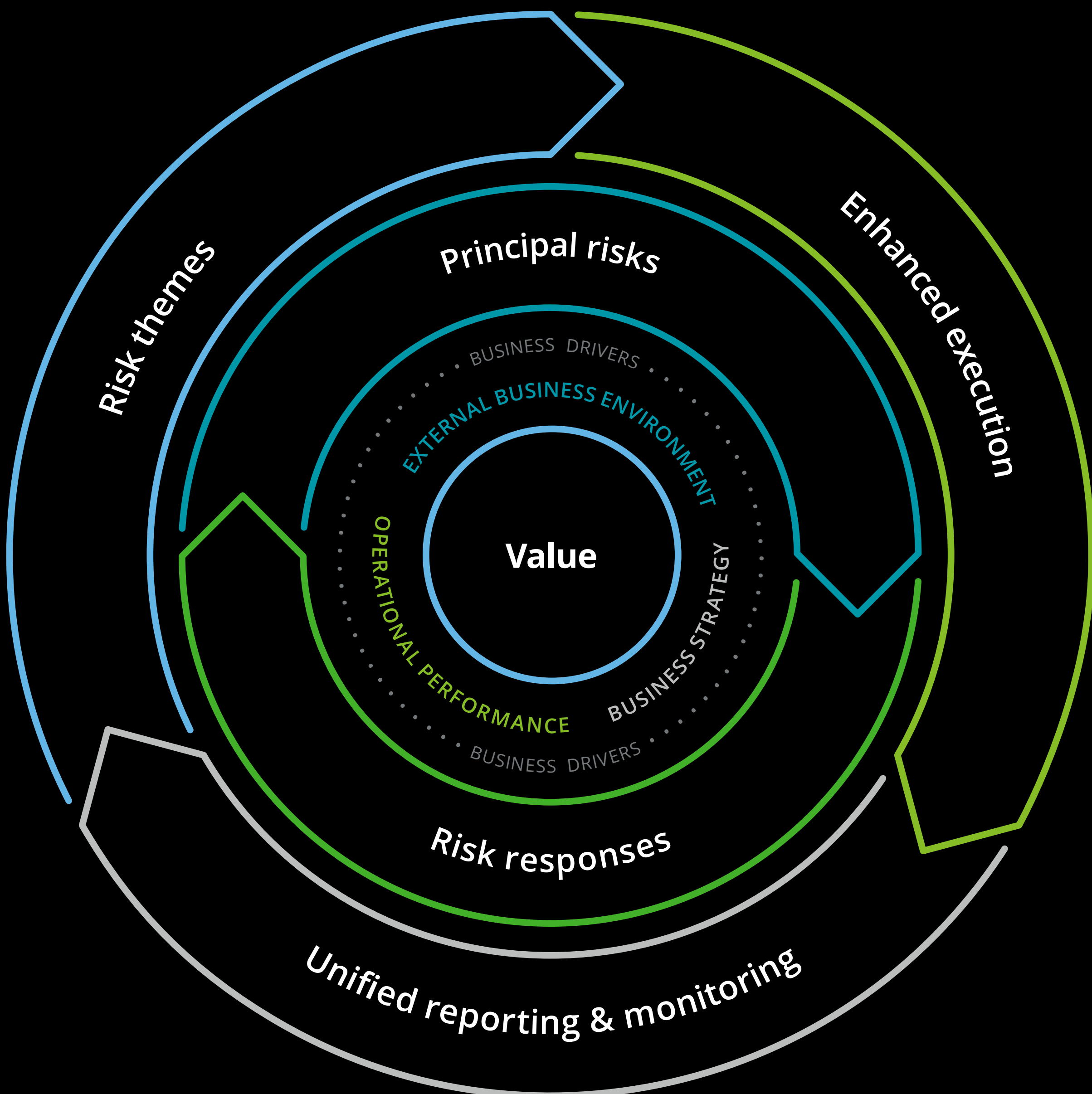
Organizing according to a new principle

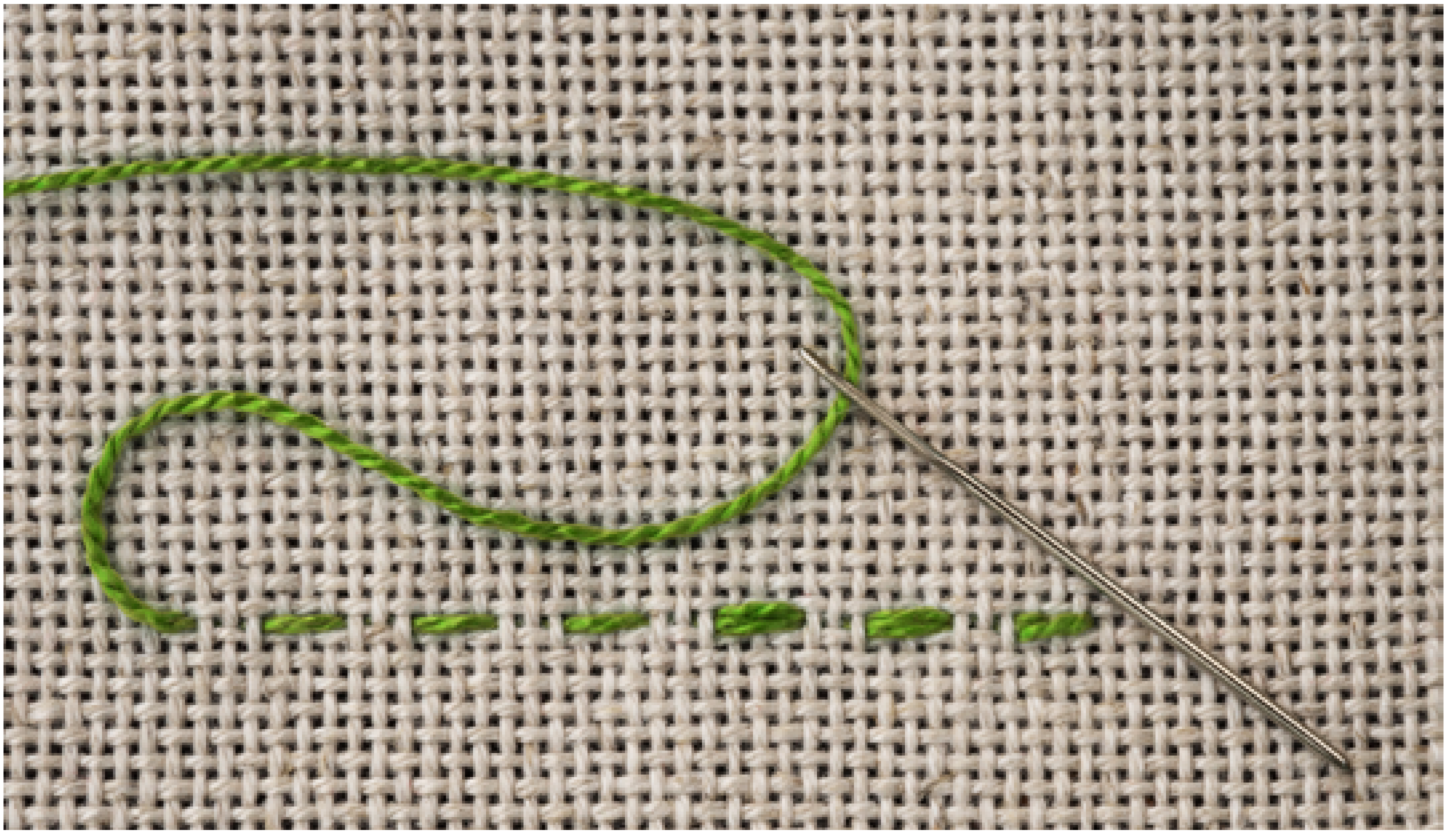
A fit-for-purpose approach to integrating risk assurance begins and ends with understanding the business drivers that preserve and enhance organizational value. Because every organization has a unique set of value drivers, each will have unique ways of defining, assessing, tracking, and addressing risks, and a unique set of processes for providing assurance.

As an organizing principle, the value drivers orient establishments toward what matters most and align risk assurance efforts to be targeted, efficient, and insightful. Once these value drivers are defined, understood, and embraced, they set the foundation for how risk assurance activities are prioritized, planned, coordinated, and delivered—and they also set the foundation for assurance reporting.

The integrated risk assurance framework summarizes this approach (Exhibit 1).

Exhibit 1: Integrated risk assurance framework



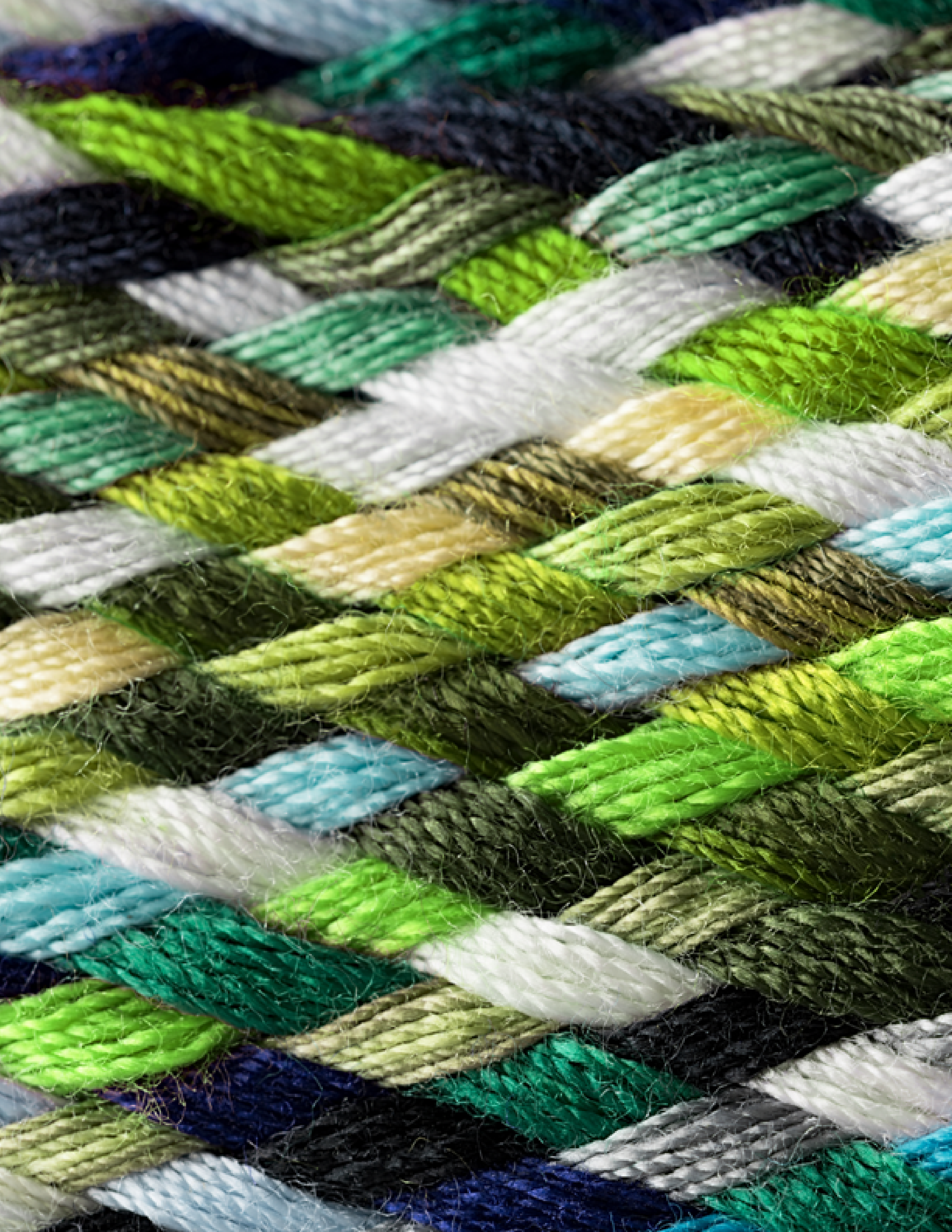


Building from the inside out, this framework provides context for aligning risk assurance with enterprise value:

Layer 1: Start with the business drivers of value To address the risks that matter most, integrated risk assurance starts with a focus on enterprise value and the business drivers of that value. These are typically shaped by a company's business strategy, operational performance, and external business environment. Each of these must be clearly defined and understood to ensure the integrated risk assurance model is organized so that risk assurance itself adds value.

Layer 2: Understand the underlying principal risks
Integrated risk assurance then identifies and assesses the risks that most jeopardize or enhance the business drivers of value; that is, those most likely to negatively or positively affect business outcomes. This analysis determines the required levels of assurance based on the organization's risk appetite and the expectations of its stakeholders—customers, partners, regulators, shareholders, and employees.

Layer 3: Plan and execute the risk assurance cycle This model of risk assurance organizes reporting around risk themes: groupings of similar or related risks that can most affect the drivers of value. Those drivers also dictate the assurance priorities that need to align with business strategy and operations. The risk themes will then guide decisions about assurance planning and execution so that resources are optimally allocated and reporting and monitoring are integrated.



Following a different assurance cycle

A compelling case for initiating integrated risk assurance can be made by examining the assurance cycle, or the outer rim of the integrated risk assurance framework. This is where risk assurance activities must be organized, resources coordinated, and reporting reimagined:

1. **Targeted risk themes for assurance planning** come primarily from framing the business drivers of value to define the risk themes that support the strategic imperatives of the enterprise. Common assurance planning on what matters can be organized in this stage. Where appropriate, information from the enterprise risk management (ERM) system and other sources may be used to enhance existing risk knowledge.
2. **Efficient, enhanced execution** requires discussion and agreement on the coordination of key risk assurance responsibilities to align levels of risk assurance to specific risk themes. This results in streamlining assurance activities within each of the defined risk themes.
3. **Insightful, unified reporting and monitoring** delivers more relevant, higher-quality risk assurance to key stakeholders with reporting that's organized by consolidated risk themes, sharing risk management and assurance methods within the organization, and monitoring the methodology and its results as the adoption of the integrated risk model evolves.

These three factors—risk themes, enhanced execution, and unified reporting and monitoring—both organize and secure the implementation of a holistic, but tailored integrated risk assurance model.

Furthermore, integrated risk assurance benefits the governance over risk by nominating a single owner for the assurance model, promoting the coordination of risk assurance forums (e.g., local, global), and by clearly linking risk assurance to management systems and quality.

Step 1

Setting context: Identifying and framing business drivers

The more critical a value driver is to the organization, the more important it is to identify, monitor, and report on the risks to that driver and on related risk management. Essentially, a shift in assurance providers' mindsets is more often needed than a radical change to assurance processes. The providers need to focus more intently on business outcomes to truly understand the assurance on risk they need to deliver.

To gain clarity on business drivers of value, a useful starting point is to focus on the factors that preserve and enhance value in the organization's industry (Exhibit 2). Each of these value drivers should be further defined to hone in on the unique factors generating risks for the company. Traditionally, assurance activities have centred on preserving value; however, the call is growing to understand risks and assurance related to the strategic and operational drivers that enhance value.

Developing a unified view of what matters most will help define and drive risk assurance activities as well as how they should be integrated, from planning through to reporting.

Exhibit 2: Framing business drivers for risk assurance (illustrative)

Shareholder value	Business drivers that preserve value	Business drivers that enhance value
Consumer & industrial products	• Product safety • Brand loyalty & reputation	• Market growth • Customer experience • Supply chain • Asset performance • Digitization
Energy & resources	• Safety • Operational integrity • Financial resiliency	• Production growth • Asset performance • Functional performance
Financial services	• Regulatory compliance • Financial resiliency • Corporate governance • Customer trust	• Sales growth • Margin optimization • Innovation via digitization • Market adaptability
Life sciences & healthcare	• Drug & device safety • Regulatory compliance • Intellectual property • Corporate governance	• Sales growth • Clinical innovation • Operating delivery model • Connected customer
Public sector	• Accountability & transparency • Privacy • Budgeting & spend integrity • Policy oversight	• Optimize service delivery • Innovation & digitization • Policy changes
Technology, media, and telecom	• Privacy • Brand & reputation • Intellectual property	• Content monetization • Customer mix • Ability to scale • Digital advancement & innovation

Step 2

Creating the platform: Linking value, business drivers, and risk themes

Assurance mapping exercises are useful for understanding the landscape of assurance activities at specific point-in-time reviews, but they can easily become overwhelming—and ultimately fail—when they try to cover all risks and organize all assurance reports simultaneously. Too often, such efforts begin with the wrong goal. The goal should be to layer in appropriate assurance on the risks that matter most to the business drivers that preserve or enhance value.

Linking business drivers to risk themes automatically organizes the risk assurance program around what matters to stakeholders. Exhibit 3 illustrates how this organizing principle operates to define and coordinate key areas of focus for risk assurance activities. This highly simplified illustration of an approach to integrated risk assurance indicates it's important that drivers of enterprise value be defined by management. This must be done at a detailed level, which means understanding the strategy, business goals, and the approach by which they will be implemented.

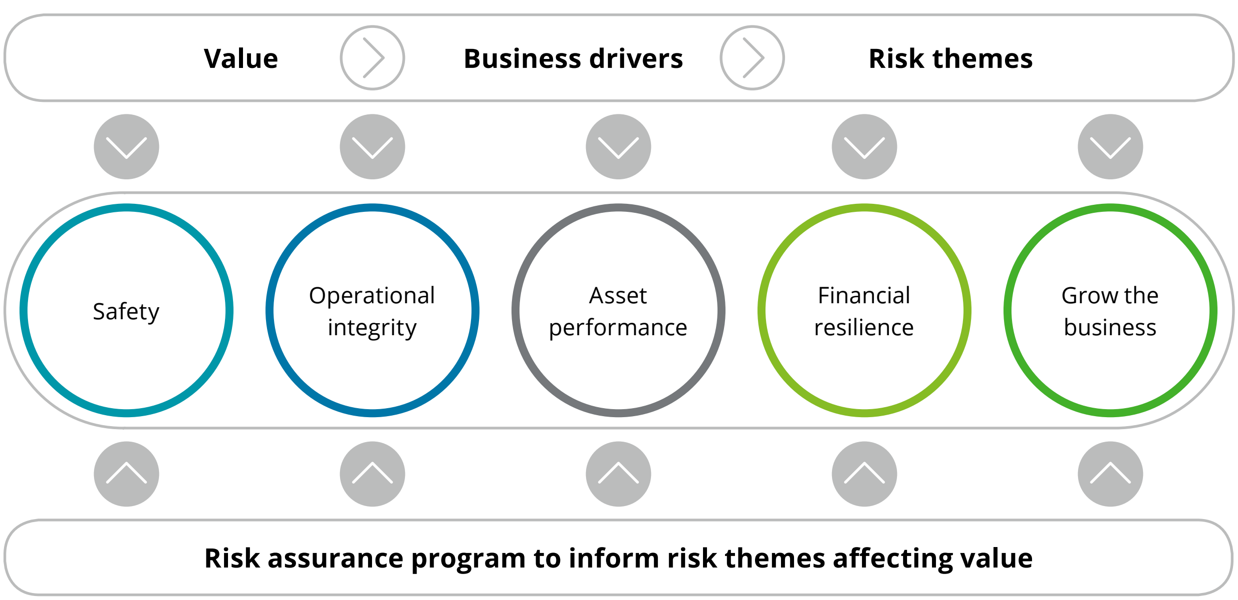
Risk themes emerge as the landscape is examined for the risks that pose the greatest threat, those that come up repeatedly, or both.

Tools such as heat maps and assessments of likelihood, impact, and velocity are useful in this process, whose objective is to develop risk themes that can be used to organize assurance in ways that:

- Focus assurance activities on the risks and risk management activities that are aligned with the organization's business drivers
- Enable each line of defence to contribute to assurance in ways that maximize efficiency and effectiveness
- Generate reports that address the most important concerns of stakeholders, and in the language of business

The risk themes direct assurance activities. They assist in setting priorities, in gauging the required level of assurance, and in deciding which line of defence can best provide that level of assurance.

Exhibit 3: Sample drivers of value and key risks



Step 3

Enhanced execution: Repositioning the three lines of defence

In contrast to many well-intentioned efforts to combine assurance, integrated risk assurance aims to dramatically simplify and coordinate the actual execution of assurance. This occurs mainly by aligning the efforts of each assurance provider to the business drivers.

As the provider of objective, independent assurance, an organization's internal audit team will either drive or play a key role in this effort. This means working with the first and second lines of defence to determine what level of assurance is needed and where it can most effectively and efficiently be provided. To execute at an enhanced level, management should consider a few key questions:

- Is the assurance framework aligned with the operating and/or organizational model?
- Are risk aggregation principles in place to support standardization across the organization?
- Is the cadence for assurance planning and execution well-coordinated?
- What technology solutions can be applied to improve coordination?

These decisions depend largely on an assessment of the level of assurance that's required, with any redundancies, overlaps, and gaps identified and addressed.

The three-lines-of-defence model has helped many organizations clarify risk responsibilities, but it has also presented challenges. In many cases, it has led to isolated functions in the second line of defence. It has sometimes left people in the first line believing risk is being managed in the second line or that they have no potential role in risk assurance. In certain instances, it has even cast internal audit as a redundant function that adds little value.

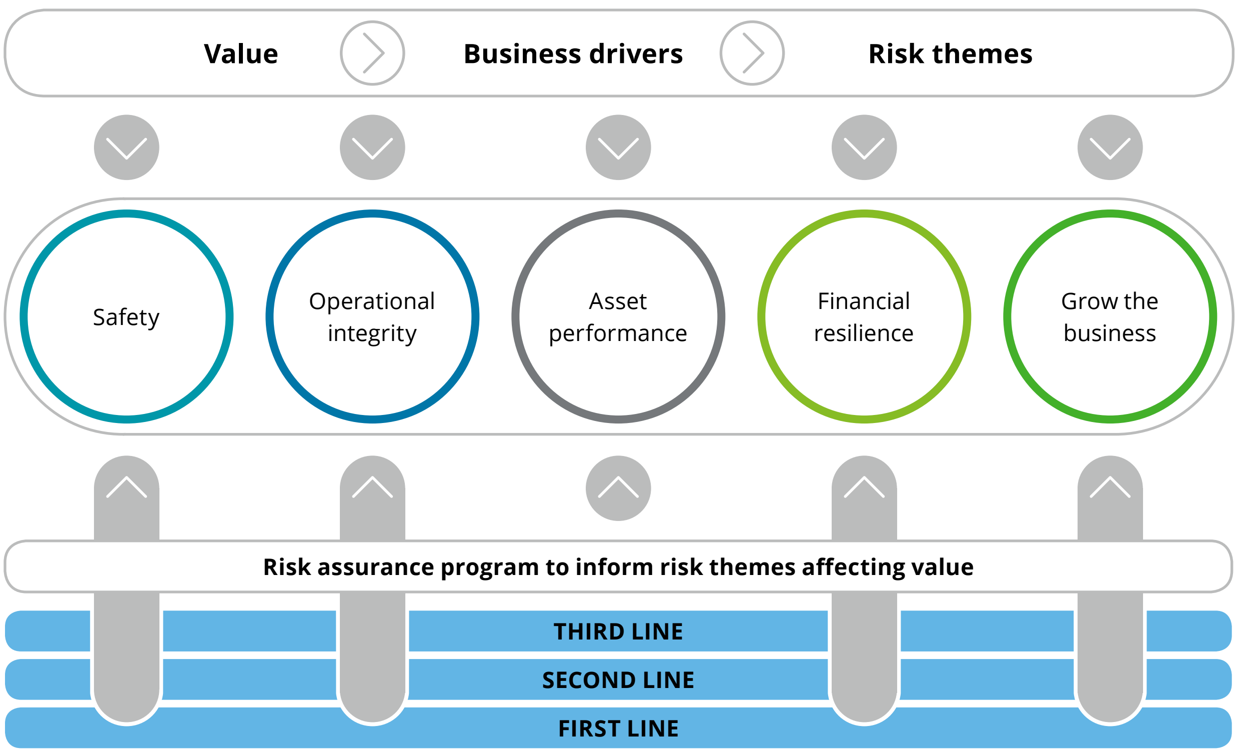
Integrated risk assurance provides an opportunity to change such situations. It's a chance to reconsider, clarify, or establish risk assurance responsibilities within the three lines. For example, day-to-day assurance responsibilities should always remain in the first line, where risks must be detected, tracked, and managed. The role of the second and third line could be based on the need for senior-level transparency and objectivity related to each risk affecting an enterprise's business value drivers. Where the need is greater, the third line of defence should play a greater role in providing assurance.

Another way could entail the second line to set standards and be business advisors, with the third line fully accountable for all assurance activities. The manner in which the risk assurance activities are deployed will have a substantial impact on its efficiency and effectiveness, and effect on the organization.

This entails redrawing the assurance map along lines dictated by the business drivers. The aim here should be to focus each relevant unit within each line on the key risks within its purview. With those lines redrawn in that way, and with assurance activities organized accordingly, a realignment of assurance reporting to the risks that stakeholders care most about will follow as a matter of course.

The assurance functions in each of the three lines of defence should focus on the goals of assurance, which are to report on the effectiveness of risk management in the areas that matter most, such as safety, operational integrity, asset performance, and so on (Exhibit 4). In the process, assurance activities and reporting should become less isolated and redundant, as activities are consolidated, used, eliminated, or enhanced within the line that can most effectively and efficiently conduct that assurance activity.

Exhibit 4: Integrating risk assurance information on risks that matter most



Step 4

Unified reporting and monitoring on the truly greatest risks

Once the stage is set and resources are aligned with the foundations of value, business drivers, and risk themes, it intuitively follows that unified reporting and monitoring is the natural next step. This is achieved in two distinct and complementary ways that enhance the depth and breadth of risk assurance reporting:

1. Integrated and coordinated reporting that uses knowledge and information within individual assurance programs improves stakeholders' understanding of how the truly greatest risks are being managed at an enterprise level. For example, where the third line can objectively leverage insights and information from assurance activities in the first and second, a more comprehensive picture on risk assurance is provided to senior management and the board.

2. Theme based reporting that utilizes cumulative knowledge acquired over a period of time to analyze assurance activities and findings along defined risk themes provides greater breath of risk assurance coverage and deeper insights into aggregate risks. Additionally, if these observations are coordinated with Enterprise Risk Management, it creates the opportunity to provide further insights on interrelated risks that need to be addressed by the enterprise.

Ultimately, reporting must focus on important business matters. These include risks to business goals and strategies and to performance and value—that is, matters related to the business drivers and risk themes. They include advice on and insights into major decisions being contemplated and initiatives currently underway—new IT installations, merger or acquisition integration, supply chain and sourcing issues, adjustments to the capital structure, and so on. They also include risk anticipation and forward-looking reports on technological, economic, competitive, regulatory, and other developments likely to affect the organization and its stakeholders.

This kind of reporting seeks to speak the language of business. It engages senior executives, the audit committee, board members, and business managers because it focuses on insights that affect their ability to succeed. It tells a story, picks up from where it left off, and leaves few questions unanswered—or at least positions assurance providers to answer them in short order.

This kind of reporting creates a new experience for assurance providers, as well as for management and the audit committee. It shows that assurance providers are doing their part to take risk management and governance to higher levels and to support management and the board in that endeavor. Over time, the accumulation of knowledge and reporting along a consistent set of risk themes informs management and the board on risk trends affecting their business drivers and further enhances their ability to make informed strategic decisions.

There's no time like the present

The specific reasons for seeking to implement integrated risk assurance may vary by the organization, but the overarching goal is to receive assurance on and insights into the truly greatest risks facing the enterprise.

The benefits of integrated risk assurance make it possible to:

Assure
with clearer, more panoramic views of all critical risks to the organization and of efforts to address them, by reducing "assurance fatigue" in business units and functions and, potentially, fewer assurance providers in the organization.

Advise
with actionable insights and advice on ways to manage these risks, build resilience, and create value, by improving the understanding on risks that impact business strategy, operational performance, and the business environment.

Anticipate
with enhanced risk anticipation and deeper insights into issues potentially affecting business decisions and initiatives, by using risk sensing technologies and other forward-looking techniques to identify and analyze emerging issues and risks.

These benefits accrue over time, but start with reconsidering the organizing principles for risk assurance in the context of the organization's underlying business drivers. They also complement the benefits of reduced costs that come with eliminating redundancies, streamlining reporting, and calibrating assurance to levels that stakeholders actually desire and need.

Benefits extend from the bottom of the organization, where risks are managed as employees perform their day-to-day jobs, to the highest levels, where senior leaders set business strategies, develop policies, and make decisions.

Integrated risk assurance enables visibility into key risks, coordination among units and functions, and ongoing monitoring that not only improves risk management and governance, but also value creation and operational performance in our increasingly risky business environments.

Contact us:

Munir Patel
Partner, Risk Advisory
Deloitte Canada
+ 1 (403) 267-0548
munirpatel@deloitte.ca

Baskaran Rajamani
Partner, Risk Advisory
Deloitte Canada
+ 1 (416) 643-8457
brajamani@deloitte.ca

Tom Rayner
Director, Risk Advisory
Deloitte Australia
+ 61 (2) 82604703
trayner@deloitte.com.au

Warren Rosenberg
Director, Risk Advisory
Deloitte Canada
+1 (514) 393-5492
warosenberg@deloitte.ca

Designed and produced by the Deloitte Design Studio, Canada. 18-5711T