

Deloitte.



Integrated Risk Management

Aligning People, Processes, and Technology



In our previous article, [Integrated Risk Management – Improving your Risk Governance Practices](#), we have highlighted how Management and Board could improve their approach on risk governance, which sets the tone for and oversees the [integrated risk management framework](#). In this current article, we would continue to explore this framework and how it could provide an enterprise-wide view of risks by bridging siloes within the traditional three lines of defense (3LOD) risk management model.

The Traditional Three Lines of Defense Model

First Line – Process Owners / Operational Management

- Forefront of identifying emerging risks in the daily operation of the business.
- Primary responsibility is to own and manage risks associated with day-to-day operational activities.
- Design, operation, and implementation of controls.

Second Line – Risk Management & Compliance

- Providing compliance and oversight in the form of frameworks, policies, tools, and techniques to support risk and compliance management.

Third Line – Audit

- Provides objective and independent assurance.
- Assess whether the first- and second-line functions are operating effectively.
- Responsible to report to the board and audit committee, in addition to providing assurance to regulators and external auditors that the control culture across the organization is effective in its design and operation.

Driven by forces such as globalization, digitalization, social media, and dependence on information technology, risks and risk events are more interrelated than ever. This continuous change affects business operations at all levels, with customers demanding real-time interactions, regulators applying increasing levels of scrutiny, and governance stakeholders requiring assurance in this complex and dynamic risk environment. The result has exposed weaknesses in the traditional three lines of defense (3LOD) risk management model.



In its current form, is the 3LOD model still relevant and efficient?

Challenges that Limit the 3LOD Model Effectiveness

To address the complex risks of an interrelated economy, the current-state 3LOD model of risk management does not provide a sufficient foundation for management decisions. An **integrated risk management** is required to bridge siloes within the 3LOD model and provides an enterprise-wide view of risks. It enables people at all lines to fulfill their risk-related responsibilities and to enable the connection of dots in the risk universe and the generation of risk intelligence and insights for management decisions.

Scenario 1

Second- and third-line functions are immature in their role, remit, and capability

Third Line

Lack of sufficient, independent, and objective assurance

Second Line

Immature second line oversight functions

First Line

An over reliance placed on management

Scenario 2

Management place too much reliance on the third line of defense

Third Line

The last line of defense is the 'primary' source of assurance

Second Line

Second-line functions are lacking effective compliance monitoring

First Line

Management lacks ownership for risk and controls; 3LOD seen as the compliance function

Scenario 3

Assurance activities are not integrated

Third Line

Assurance efforts are duplicated

Second Line

The business is overly disrupted from uncoordinated assurance activities and siloed

First Line

Value is left on the table; potential efficiencies and strategic approaches to digital, integrated assurance models are fragmented

Integrated Risk Management

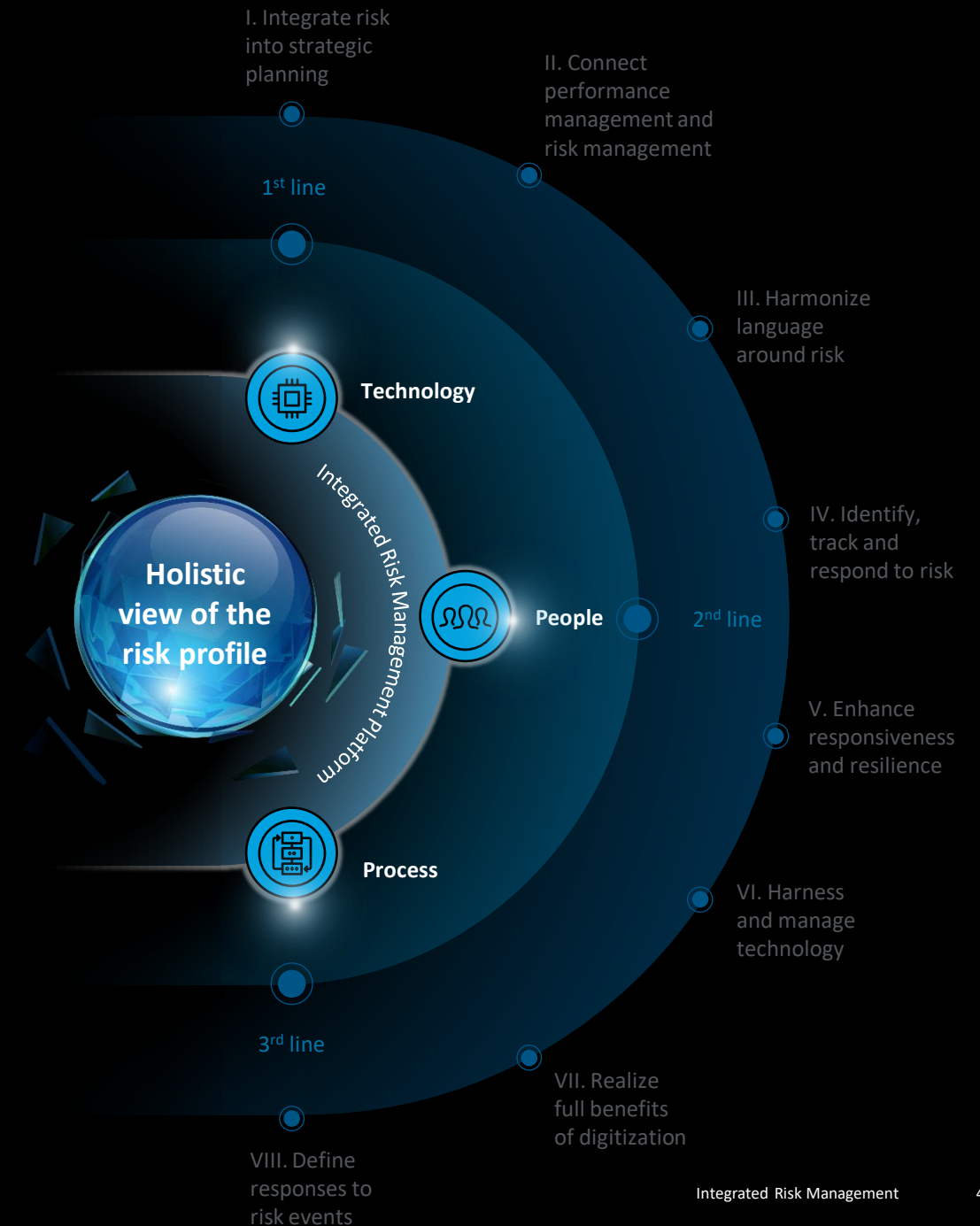
Aligning people, processes, and technology.

Integrated risk management (“IRM”) is the totality of the risk management processes, tools, technologies, methodologies, and reporting mechanisms, and it enables people to put those elements into action more rapidly, effectively, and economically.

From the people perspective, this means leveraging business, functional, and risk managers’ expertise in the design of the platform. In addition, the platform establishes a feedback loop in which people in the three lines model assess outcomes of decisions and responses and use lessons learned to modify the platform.

From the process perspective, this entails establishing data flows parallel to the processes that address risks in keeping with the organization’s desired risk profile, risk appetite, and risk tolerances. The platform supports the processes that assist management in achieving strategic goals while enabling them to better fulfill their risk governance and risk management responsibilities.

From the technology perspective, systems of data capture, analysis, and distribution deliver the right information to the right people at the right time. For example, data visualization technologies enable dashboards that can signal emerging risks, likely outcomes, and potential responses under various scenarios. Today’s technologies can also lower the barriers posed by legacy systems while preserving the organization’s investment in those systems.



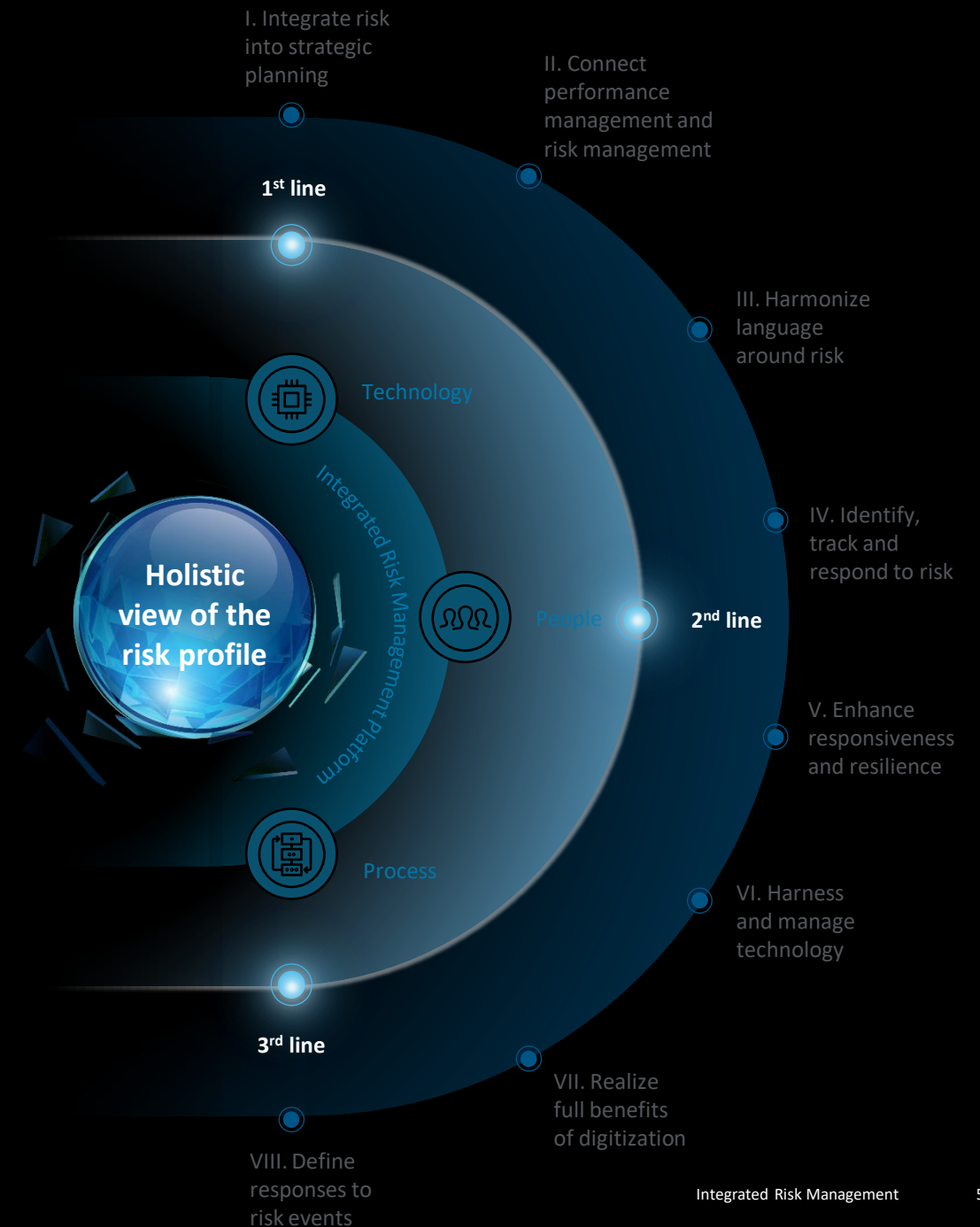
Integrated Risk Management (Cont'd)

Operationalizes the 3 lines of defense model.

IRM links the business strategy with the risk strategy and improves performance in that it operationalizes the 3LOD model of risk management by:

- Providing the **first line**, which owns and manages risk, with relevant, timely, actionable information and insights.
- Enabling the **second line**, which supports the first line, to provide better support and proactive guidance to the business.
- Positioning the **third line**, internal audit, to more effectively allocate assurance resources and move toward automated assurance.

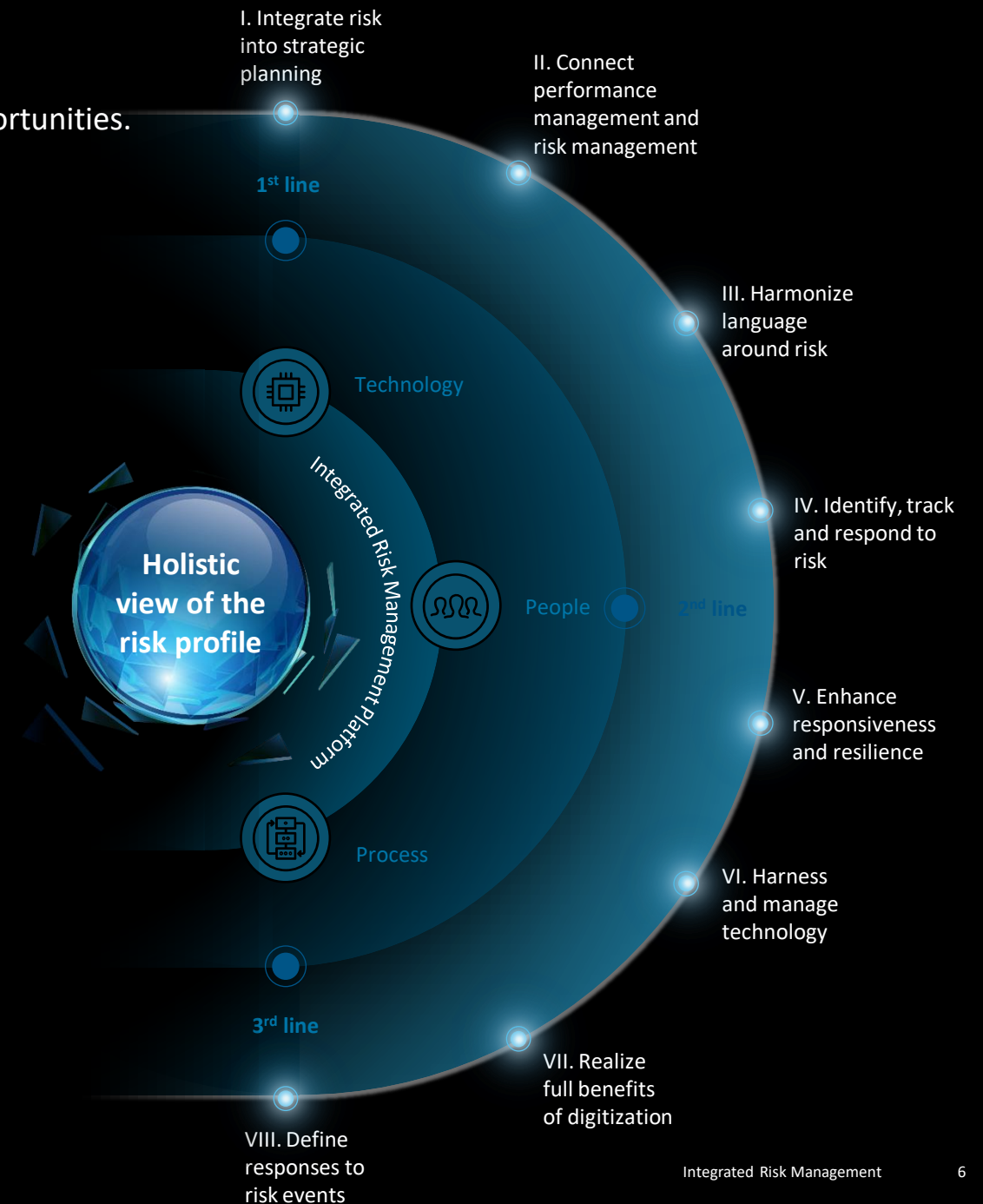
By integrating risk management with planning, forecasting, performance measurement, and other systems, the platform illuminates relationships between risk management and performance management. It enables management to identify risks to drivers of value, even at the level of the profit and loss statement, and to optimize risk positions. This in turn drives performance and profitability through informed risk taking and proactively limiting losses across risk categories.



Integrated Risk Management (Cont'd)

Presents business, financial, operational, and risk managers with valuable opportunities.

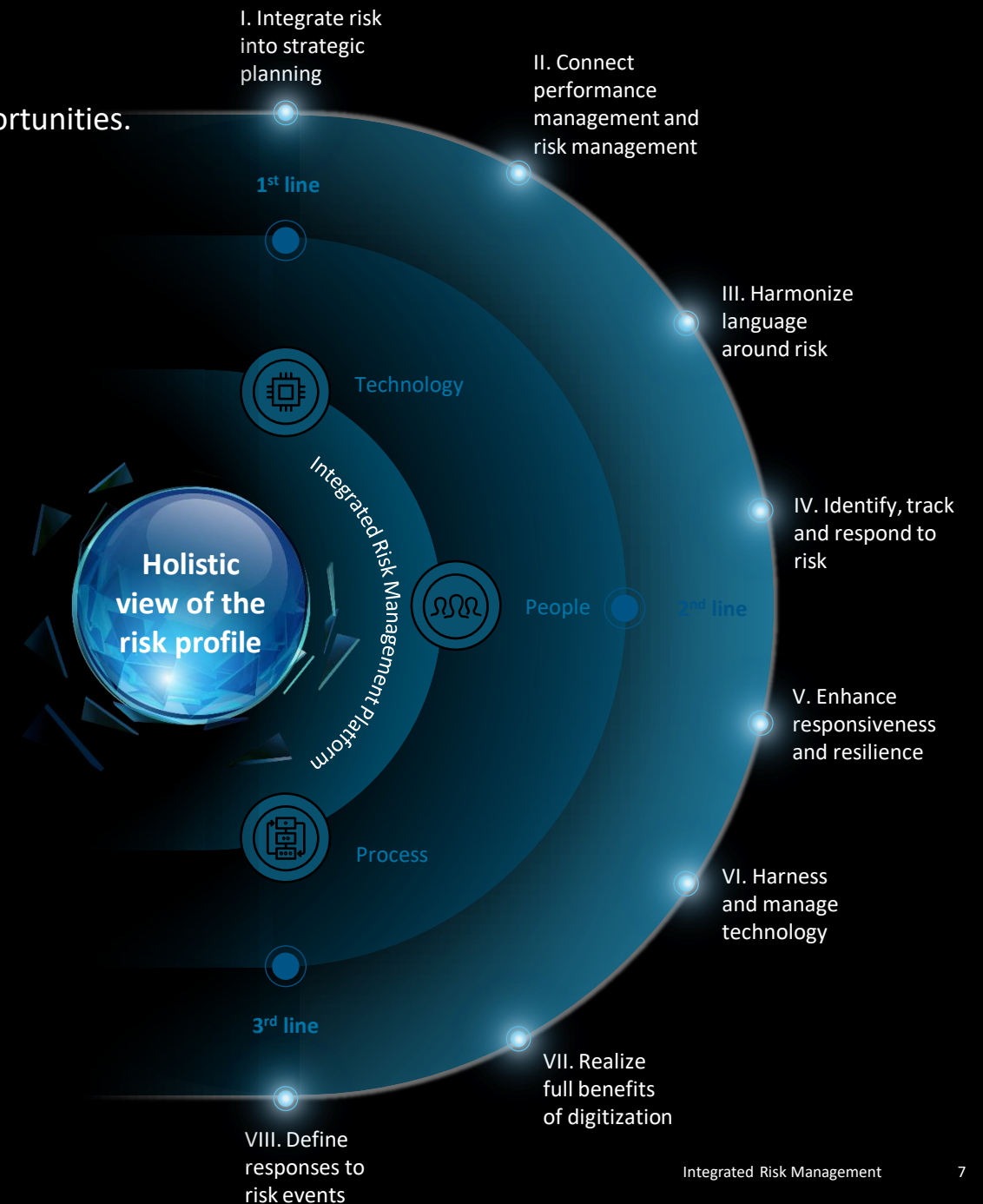
- I. **Integrate risk into strategic planning** – Senior leaders must consider risks to the strategy, risks of the strategy, and risks posed by incorrect assumptions underlying the strategy. The right risk platform can enable management to more explicitly consider these factors and thus integrate risk more fully into strategic planning—and into real-time course corrections. With this capability, management can more quickly adjust risk appetite, tolerances, and positions to achieve greater agility and enhanced resilience when faced with volatility.
- II. **Connect performance management and risk management** – In many organizations, performance management is not connected to risk management. People’s business or functional performance is often evaluated without consideration of their performance of risk-related responsibilities. At times, people in the first line—the business—believe that risk is being managed in the second line by a “risk management” function. An integrated platform rests on the premise that performance management and risk management are aligned.
- III. **Harmonize language around risk** – Lack of a shared language of risk and common risk measures can undermine evaluations of risks and impacts. A common taxonomy of risk facilitates those evaluations as well as communication about risk, and it can help to improve controls. Harmonizing language and measures fosters a consistent approach to risk and contributes to a functioning IRM.
- IV. **Identify, track, and respond to risk** – First-line personnel need timely information on evolving risk positions, emerging threats, and useful mitigation steps. Senior managers need up-to-date intelligence on a broad range of risks and potential responses and likely outcomes. IRM can provide the scanning, analytical, and reporting capabilities required to meet these needs.



Integrated Risk Management (Cont'd)

Presents business, financial, operational, and risk managers with valuable opportunities.

- V. **Enhance responsiveness and resilience** – No organization is immune to value-destroying events. When such an event occurs, stakeholders scrutinize the leadership’s response and the organization’s resilience— its ability to rapidly return to fully operational capabilities. IRM can help management to anticipate impacts, gauge knock-on effects, and craft clear communications to all stakeholders, while accelerating responses and reinforcing resilience.
- VI. **Harness—and manage—technology** – Technology powers IRM. However, many companies have legacy systems that would be expensive to replace. Automated tools can facilitate data aggregation and management and bridge silos while leaving legacy systems largely intact. Also, technology itself presents risks beyond cyber risks, such as competitors using new technologies to disrupt business models and leaders facing the need to place “technology bets” in an uncertain environment. IRM can help management to address such risks.
- VII. **Realize full benefits of digitalization** – The data gathering, analysis, and distribution capabilities of IRM enables the organization to make digitalization of risk management a reality. For example, it can enable real-time risk monitoring, predictive analytics, and application of artificial intelligence (“AI”) to scanning and analysis of unstructured data from diverse sources. AI can be used to analyze trends and patterns to identify and track emerging risks and opportunities in a range of situations, from forecasting equipment failures to monitoring organizational culture.
- VIII. **Define responses to risk events** – IRM should incorporate the results of scenario planning, war gaming, and response exercises. Root cause analysis and other process improvement methodologies can improve responses and resilience as well as day-to-day practices. Risk escalation guidelines and response playbooks for people at all levels—and for extended enterprise partners—can further enhance resilience. Each of these can be improved through IRM.



Embarking IRM Journey

A leadership team might consider the following initial steps in developing an IRM:

Understand stakeholders' needs and expectations

Different stakeholders will have different needs for risk information and various ways of using it.

Create an inventory of risk data

Integrating risk data calls for identifying all sources of data relevant to the strategic, operational, financial, health and safety, regulatory, legal, cyber, ESG, reputational, and other risks the organization faces.

Define use cases for the risk platform

Typical cases might include monitoring specific types of risk, such as third-party risk, risk reporting to the C-suite and board, and automating assurance.

Create a blueprint

The people, processes, and technology that will comprise the platform should be mapped into a "blueprint" showing the role these resources will play and how they will fit together.

Commit to building a risk-informed culture

Ultimately, the success of this initiative depends on the people using the information, assessing the risks, and executing the responses. Therefore, senior leaders need to maintain a culture in which people at all levels see the importance of risk management.

How we help

How an organization starts constructing its integrated risk management largely depends on the current state of its risk management and risk information infrastructure. Wherever your organization is on its journey to integrated risk management, we are here to assist you.

Get in touch



Cheryl Lim
Executive Director
Deloitte Risk Advisory
cherylim@deloitte.com



Lim Kim Hwee
Executive Director
Deloitte Risk Advisory
kimhlim@deloitte.com



Andy Wee
Director (Governance)
Deloitte Risk Advisory
awe@deloitte.com



Richard Chung
Director (Enterprise Risk Management)
Deloitte Risk Advisory
cherchung@deloitte.com



Lim Thien Hui
Manager (Enterprise Risk Management)
Deloitte Risk Advisory
thlim@deloitte.com



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

About Deloitte Singapore

In Singapore, risk advisory services are provided by Deloitte & Touche Enterprise Risk Services Pte. Ltd. and other services (where applicable) may be carried out by its subsidiaries and/or affiliates. Deloitte & Touche Enterprise Risk Services Pte. Ltd. (Unique entity number: 197800820D) is a company registered with the Accounting and Corporate Regulatory Authority of Singapore.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) 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 representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

© 2023 Deloitte & Touche Enterprise Risk Services Pte. Ltd

Designed by CoRe Creative Services. RITM1488233