Deloitte.

Creating a Risk Intelligent infrastructure

Getting Risk Intelligence done

Risk Intelligence series

Contents

Preface

This publication is part of Deloitte's series on Risk Intelligence — a risk management philosophy that focuses not solely on risk avoidance and mitigation, but also on risk-taking as a means to value creation. The concepts and viewpoints presented here build upon and complement other publications in the series that span roles, industries, and business issues. To access all the white papers in the Risk Intelligence series, visit: www.deloitte.com/risk.

Open communication is a key characteristic of the Risk Intelligent Enterprise™. We encourage you to share this white paper with your colleagues — executives, board members, and key managers at your company. The issues outlined herein will serve as useful points to consider and discuss in the continuing effort to increase your company's Risk Intelligence.

Introduction

Most business leaders today understand what risk management is and why it's important — but they're still wrestling with questions about how to make it work in real life. What does your organization need to do to manage risk effectively? Who should be responsible for what? What tools and technologies do they need? Questions like these, and finding effective answers to them, are at the heart of the challenge of creating the "right" risk management infrastructure to make your organization a Risk Intelligent Enterprise.

This paper, based on a Deloitte Dbriefs presentation titled "Creating a Risk Intelligent Infrastructure," gives our most current thinking on building effective risk management practices into the fabric of your organization. We hope that you find these ideas useful in furthering your pursuit of creating a Risk Intelligent Enterprise.

This paper presents information and polling data from Deloitte's Dbriefs for Financial Executives webcast series, Creating a Risk Intelligent Infrastructure: Enhancing Enterprise-Wide Risk Management Characteristics, held on December 17, 2009, with Deloitte & Touche LLP Partner Sandy Pundmann and Deloitte Consulting LLP Principal Michael Fuchs presenting. Total webcast attendance: approximately 1,750 participants, including CFOs, directors, finance managers, analysts, auditors, and other financial executives. Polling results presented herein are solely the thoughts and opinions of the webcast participants' and are not necessarily representative of the total population of all financial executives. However, we believe the results do provide valuable insight regarding the opinions and concerns of financial executives in general as the results are consistent with the experiences of Deloitte practitioners who have worked on related engagements with numerous companies.

The Risk Intelligent Enterprise: A quick recap

A Risk Intelligent Enterprise views calculated risk-taking as essential to value creation, since virtually any activity that seeks to increase value also carries some degree of risk. Understanding that risk is integral to the pursuit of value, a Risk Intelligent Enterprise does not strive to eliminate risk or even always to minimize it — a perspective that represents a critical change from the traditional view of risk as something to avoid. Rather, a Risk Intelligent Enterprise seeks to manage risk exposures across all parts of the organization so that, at any given time, it incurs just enough of the right kinds of risk — no more, no less — to effectively pursue its strategic goals.

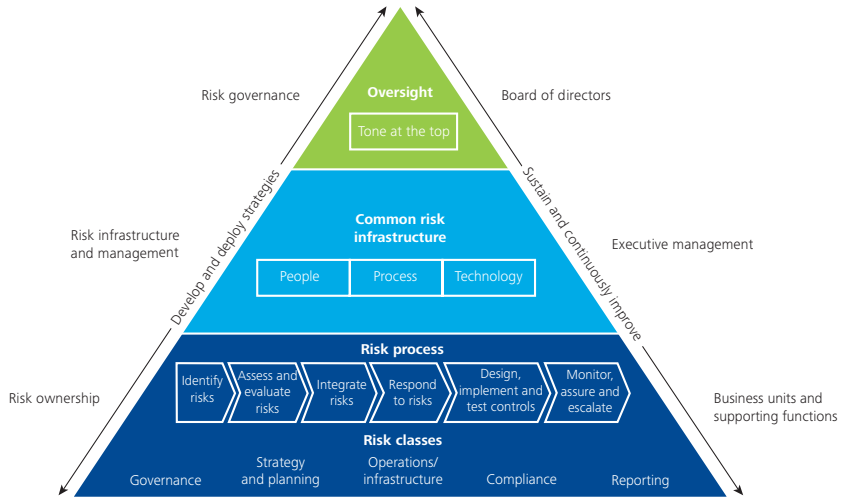
To maintain alignment between risk exposures and business strategy, a Risk Intelligent Enterprise draws on the coordinated efforts of three levels of risk management responsibility, graphically represented as a three-layered triangle in Deloitte's Risk Intelligent Enterprise framework (Figure 1):

- Risk *governance*, including strategic decision-making and risk oversight, led by the board of directors
- Risk *infrastructure and management*, including designing, implementing, and maintaining an effective risk management program, led by executive management
- Risk *ownership*, including identifying, measuring, monitoring, and reporting on specific risks, led by the business units and functions

The Risk Intelligent Enterprise is an organization that:

- Understands that both value and risk are key to enterprise management
- Understands that risk management must be built into the core ways of protecting existing assets and of creating future value
- Assumes turbulence is inevitable and emphasizes prevention and preparedness to improve both resilience and agility
- Is vigilant for a broad range of opportunities and risks across the enterprise
- Acknowledges the need for specialization by business function, as well as the need to harmonize, synchronize, and rationalize risk management and controls
- Considers interactions among multiple risks rather than focusing on a single risk or event, and considers the impacts that could result from multiple threats
- Creates a common language of terms and metrics for value and risk, and a culture in which people account for value and risk in every key decision and activity
- Encourages informed risk taking for reward and value creation, rather than pure risk avoidance

Figure 1. The Risk Intelligent Enterprise framework



The top level, risk governance, *directs* the Risk Intelligent Enterprise. It defines the parameters of acceptable risk, monitors strategic alignment, and sets overall risk management expectations. The bottom level of risk ownership, in turn, is what risk governance relies on to *execute* Risk Intelligence. It includes all of the functions' and business units' responsibilities with regard to identifying, evaluating, mitigating, and responding to risks in accordance with risk governance mandates.

The middle level, risk infrastructure and management, forms the essential link between risk governance and risk ownership. Composed of the three "pillars" of people, process, and technology, we believe that an effective "common" risk management infrastructure — that is, an infrastructure that supports consistent risk management approaches throughout the organization — is essential to the ability to give executive management an enterprise-wide view of risk, particularly across four key areas:

- Strategic risks: risks both to and of the organization's strategic objectives, identified by the C-suite with the concurrence of the board
- Operational risks: major risks that affect the organization's ability to execute the strategic plan
- Financial risks: risks in areas including financial reporting, valuation, market, liquidity, and credit risks
- Compliance risks: risks related to legal and regulatory compliance

Why do companies need a common risk management infrastructure?

Most companies already have a multitude of risk management processes that address specific risks within particular organizational areas — functional risks, business-unit-specific risks, compliance risks, and so on. However, while these processes may effectively address the specific risks they target, a company that lacks an overarching risk management approach to coordinate these activities may experience risk management gaps and redundancies, and often also lacks insight into key risk interdependencies.

A common risk management infrastructure can serve as the "glue" that gives cohesion and consistency to an organization's individual risk management efforts. It can give leaders an integrated view of risk from across the organization, help decision-makers identify and address interdependencies among risks, help reduce inefficiencies and redundancies, and help drive consistent treatment of risks throughout the enterprise. By doing so, an effective common risk management infrastructure helps to enable Risk Intelligent enterprise management — the ability to incorporate Risk Intelligence into every decision, practice, and initiative that the organization undertakes.[1]

A Risk Intelligent infrastructure bridges organizational silos to help the organization in its efforts to:

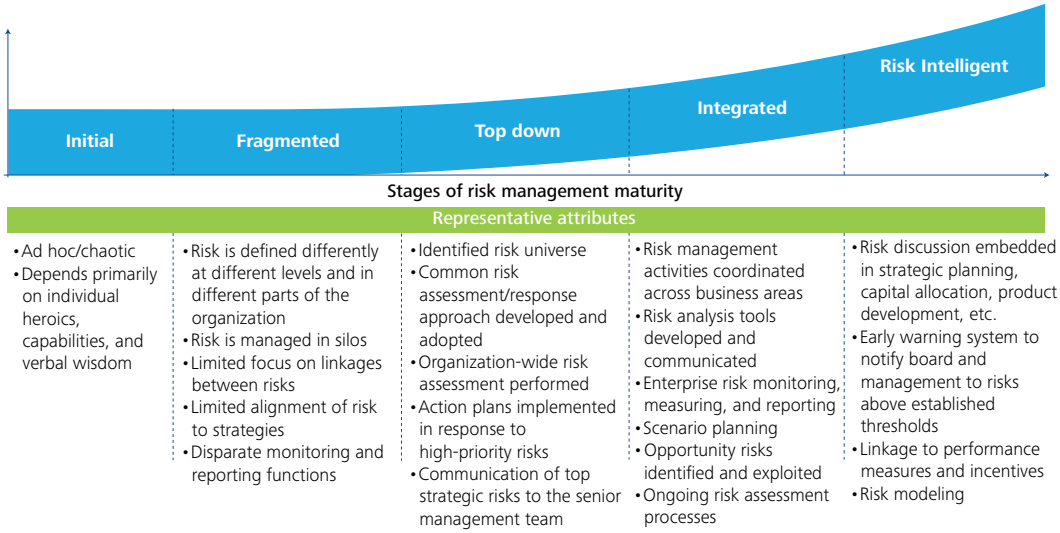
- Synchronize — coordinate risk management across institutional boundaries
- Harmonize — help risk managers all speak the same language and define risk in the same manner
- Rationalize — eliminate duplication of effort

The goals of a common risk management infrastructure include:

- Get everyone "singing from the same song sheet"
  - Constrain, guide, or channel behaviors in ways that align with the goals, strategies, and tactics established by management and the board
- Create the ability to manage risk exposures so that the organization can take enough of the right risks to pursue its strategic goals
- Create "risk aware" thinking and decision making at all levels
- Enable appropriate flows of risk information up, down, and across the organization
- Enable and support management of risks at the appropriate level

[1] Frederick Funston and Stephen Wagner, *Surviving and Thriving in Uncertainty: Creating the Risk Intelligent Enterprise*, New York: John Wiley & Sons, Inc., 2010.

Figure 2. Risk Intelligence maturity model



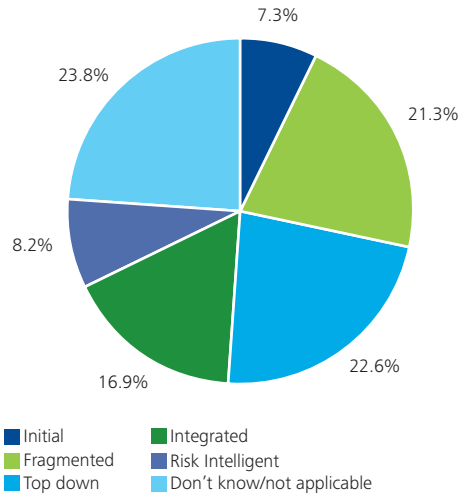
A maturity model for Risk Intelligence

We have found the maturity model illustrated in Figure 2 to be a useful tool for organizations seeking to understand their current situation and the steps they might consider to move forward in their journey toward Risk Intelligence. As organizations progress along the maturity curve, their risk management activities become steadily more integrated and coordinated, and risk becomes more of a strategic concern that is embedded into leadership's planning processes and into the organization's day-to-day business activities.

Figure 3. Deloitte executive poll results: Risk infrastructure capability

How would you rate your organization's current risk infrastructure capability?

Votes received: 1,541



Pillar one: Process

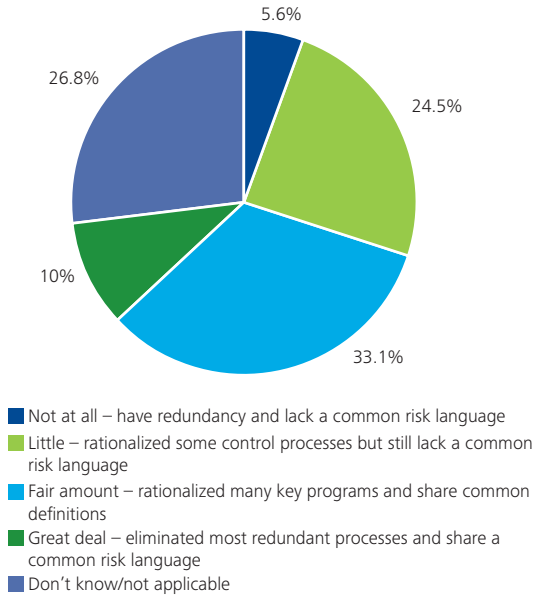
In the context of a Risk Intelligent infrastructure, establishing "common" risk management processes does not mean forcing identical processes onto all of the groups that manage risk in an organization (see sidebar, "Sample common risk management constituents"). Rather, it means finding and taking advantage of common process elements where applicable and appropriate in order to remove redundancies, improve efficiency, and reduce duplication of effort. It also means establishing processes for pushing down a unified view of risk — standardized risk definitions, a common risk language, and so on — from the risk governance bodies to all parts of the organization. And finally, it means setting up processes for consolidating risk information from different groups, effectively sharing it across the enterprise, and presenting an integrated view of organizational risks to leadership.

Sample common risk management constituents:

- Finance — Internal control, capital, disclosure, credit, liquidity, commodity, risk analytics and modeling
- Tax — Global, domestic, and cross-jurisdictional tax compliance, reporting, and examination risks related to income, franchise, indirect, property, excise and payroll taxes
- General counsel — Legal and intellectual property
- Information management — IT security, data integrity, privacy, information adequacy, business process/continuity risks
- Compliance and ethics — Ethics and business conduct, regulatory compliance risks
- Internal audit — Risk-informed audits, risks to internal control, key exposures and vulnerabilities, assurance
- Strategic planning and business development — Market and strategic risks
- Security — Risks to property and people
- Insurance — Property, casualty, liability, and hazards
- Operations — Quality of care, customer relations, market and pricing, competitive, people/process/asset performance, environmental and safety risks

Figure 4. Deloitte executive poll results: Process
To what extent has your organization implemented "common" risk management processes?

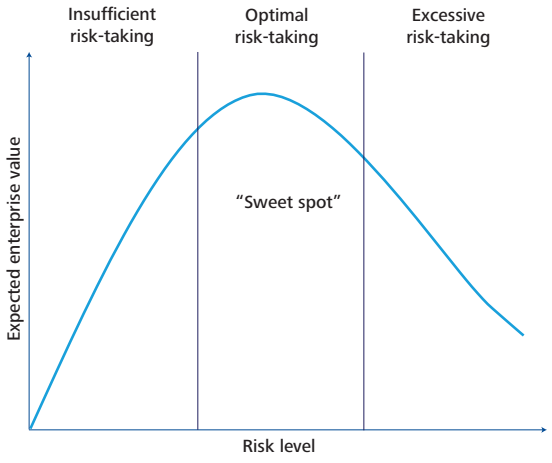
Votes received: 1,567



We recommend that organizations establish an oversight structure for the risk program that delineates clearly defined roles and responsibilities as to who performs which risk management tasks. One possible such structure is depicted in Figure 5. The risk oversight structure should include program structure and execution with the aim of establishing a program with clear, consistent processes that help keep the organization firmly within its risk tolerance — that is, the amount of risk, broadly defined, that the organization is willing to accept to achieve business objectives (Figure 6).

Figure 5. Typical roles and responsibilities for risk oversight

Figure 6. Risk tolerance: Hitting the sweet spot



In our view, risk management and risk oversight processes are most effective when they are integrated into "normal" business processes rather than layered on top as a distinct additional activity. At the most granular level, appropriate risk management activities — executing controls, gathering and reporting information, and so on — should be built into every relevant business process as part of the routine, and the corresponding responsibilities built into the job descriptions of all personnel involved. And on a higher level, all decision-making processes should incorporate, as part of the process, activities designed to appropriately consider and evaluate the risks associated with each decision. In our experience, the greater the integration between risk and business processes, the easier it is to make Risk Intelligence sustainable at every level of the organization, from boards and senior management down to the rank and file.

Pillar two: People

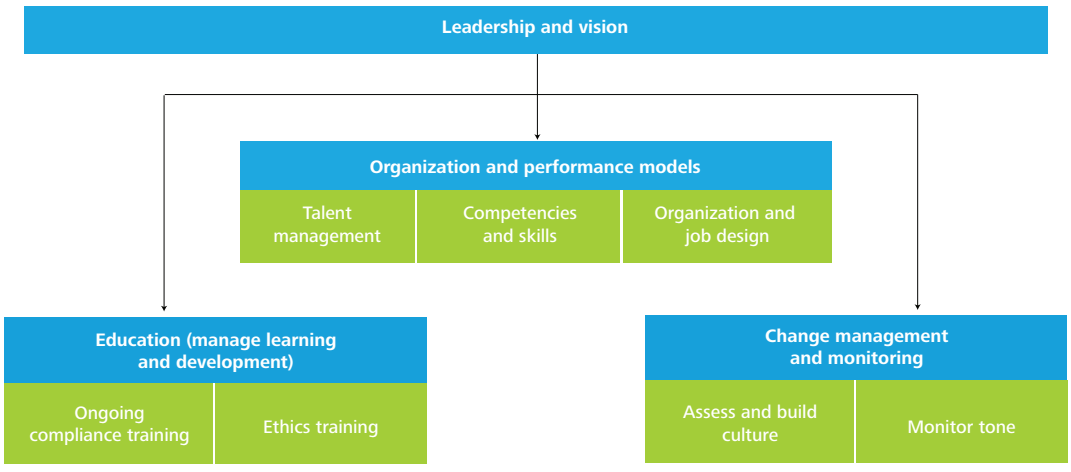
The goal of a Risk Intelligent people infrastructure is to both make it possible and desirable to do what is necessary to accomplish the organization's risk management objectives. While commonality of process can make it easier for people to execute a Risk Intelligent vision, effective processes need to be buttressed by role-based training, risk-aligned compensation and rewards, and a risk-aware culture in order to sustain Risk Intelligence for the long term. The objective is to help people everywhere in the organization understand why they need to make decisions about risk and what risk-related decisions they need to make; to give them the tools and training to make Risk Intelligent decisions; and to help them understand how they themselves will be rewarded for Risk Intelligent behavior.

We suggest an accountability model for risk management (Figure 7) that is based on:

- ***A strong leadership vision.*** It is easy for leaders to say that risk is important, but it's vital to back up those statements with appropriate investments and changes to operations so that employees understand that leaders are truly behind the pursuit of Risk Intelligence. Leaders should establish a strong "tone at the top" by setting a clear and forceful vision, just as they would do with any new strategy that the organization is undertaking.
- ***Well-defined organization and performance models.*** Once the leadership vision is established, the next step is to establish organization and performance models so that people throughout the organization understand what they need to do with regard to risk and are appropriately rewarded for doing it. In particular, misaligned compensation and rewards structures can be enormously detrimental to Risk Intelligence.
- ***Role-based risk management education.*** Most organizations maintain relatively strong training programs in functions that are explicitly focused on risk management, such as legal, internal audit, and the various compliance functions. The challenge for many organizations is to establish a learning and development program that identifies risk management training needs for people outside the formal risk management functions and delivers the training in a way that is specific to each person's role. Especially challenging can be to account for the way training needs change as a person moves to different roles in the organization.
- ***Change management and cultural monitoring.*** Setting a strong tone at the top through advocacy and communication is key to establishing a Risk Intelligent culture. Formal cultural assessments can help boards and executives monitor cultural alignment and alert them to any potential need for intervention.

These components lay the foundation for creating a solid people infrastructure and an operating environment that supports ongoing risk management and good overall enterprise governance.

Figure 7. Building an effective accountability model



Questions to ask about an organization's people infrastructure:

Organizational design

- Do you have the right structure in place to manage risk on an ongoing basis?
- Are your risk management resources being used efficiently?

Roles and responsibilities

- Are your roles for risk management well-defined?
- Do your people understand what their risk management responsibilities are?

Talent management

- Do you have enough people to do what needs to be done to effectively manage risk?
- Do those people have the right skills to help support effective risk management execution?

Training and development

- Do you have mechanisms in place to train and measure risk-related skills and knowledge?
- Have risk management competencies been embedded into your competency model?

Measurement and reward

- How will you measure performance and reward desired risk management behavior?

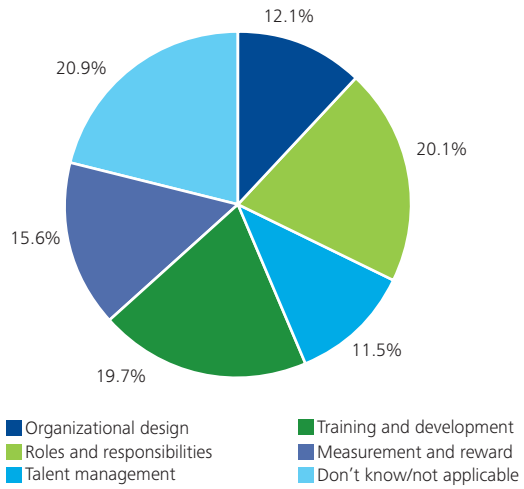
Recommended tasks for sustaining the people component of Risk Intelligence include:

- ***Formalize the risk management, compliance, and governance issue.*** Activities include forming committees, teams, offices, and other organizational structures around risk-related activities.
- ***Define roles and responsibilities.*** The more deeply the philosophy of strong risk management is embedded, the more sustainable Risk Intelligence becomes.
- ***Identify needed skills and competencies.*** Risk management can be a highly specialized subject; staff focused on risk management should be properly trained in the required skill sets.
- ***Create a staff development strategy and supporting plans.*** Monitor recruiting activities, corporate philosophy, budgets, and other factors to develop a strategy to help maintain staff competency.
- ***Link employee performance to reward and recognition systems.*** Promote and embed desired risk management behaviors into the existing culture by leveraging existing reward systems.

Above all, sustaining the people component of Risk Intelligence must be an ongoing effort, not a one-time activity. The roles, responsibilities, training, and culture needed for Risk Intelligence must be built into the organization's operating model, its competency model, its training and development programs, and its compensation and rewards structures, all geared toward giving people the tools, skills, and motivation to "do the right thing."[2]

Figure 8. Deloitte executive poll results: People
What do you believe is your organization's greatest challenge pertaining to the people pillar of risk infrastructure?

Votes received: 1,525



[2] For a broader discussion of the relationship between talent and risk management, see "The people side of Risk Intelligence: Aligning talent and risk management," Deloitte Development LLC, 2010. Available online at http://www.deloitte.com/view/en_US/us/Insights/browse-by-role/Chief-Human-Resources-Officer-CHRO/617529bbdb177210VgnVCM100000ba42f00aRCRD.htm.

Pillar three: Information technology

Information technology (IT) plays a crucial role in assisting organizations to manage their risks. Importantly, it is not a substitute for weak governance, ineffective processes, or insufficiently skilled and trained people — but with the right governance, process, and people elements in place, technology can make a significant difference in the effectiveness and efficiency of an organization's Risk Intelligence program.

Leaving aside consideration of highly specialized tools for analyzing specific risks (such as those used by the banking and insurance industries), the main role of an overarching IT infrastructure for risk management is to deliver the right type and amount of information to the right people in a timely manner, distilled in a way that can help them understand the risk associated with particular decisions. To this end, technology can provide support by:

- Delivering a high-quality, reliable continuum of information from dispersed operations
- Integrating operational, transactional and financial information to help in proactively identifying and resolving risk-related issues
- Predicting, preventing, detecting, managing and reporting both internal and external risks that may otherwise stealthily or overtly threaten an organization's ability to fulfill its business objectives
- Creating consistency and transparency of real-time information across the enterprise

We envision an IT infrastructure organized into five components, or "layers," that can support the integration of people and processes across a common risk architecture (Figure 9):

- ***Consolidated reporting layer.*** The consolidated reporting layer provides information that enables boards, executives, and management to govern compliance, risk, and performance, providing indicators that monitor the support for a successful Risk Intelligent entity.
- ***Management layer.*** The management layer provides the foundation for an effective and efficient risk program. It allows the company to support the governance, risk, and compliance environment from different views to meet multiple needs — including the opportunity to streamline controls when appropriate.
- ***Business process layer.*** The business process layer connects isolated business functions and orchestrates them into cohesive business processes. This layer includes business process integration, business process management, and business activity monitoring.
- ***Control monitoring and testing layer.*** The control layer is where the actual control activities are performed. This layer includes the automation and monitoring components that provide for increased reliability, efficiency, and real-time decision support.
- ***The foundation and transaction source layer.*** This layer consists of the applications and protocols that manage data and communication across the enterprise.

Figure 9. Risk management IT infrastructure

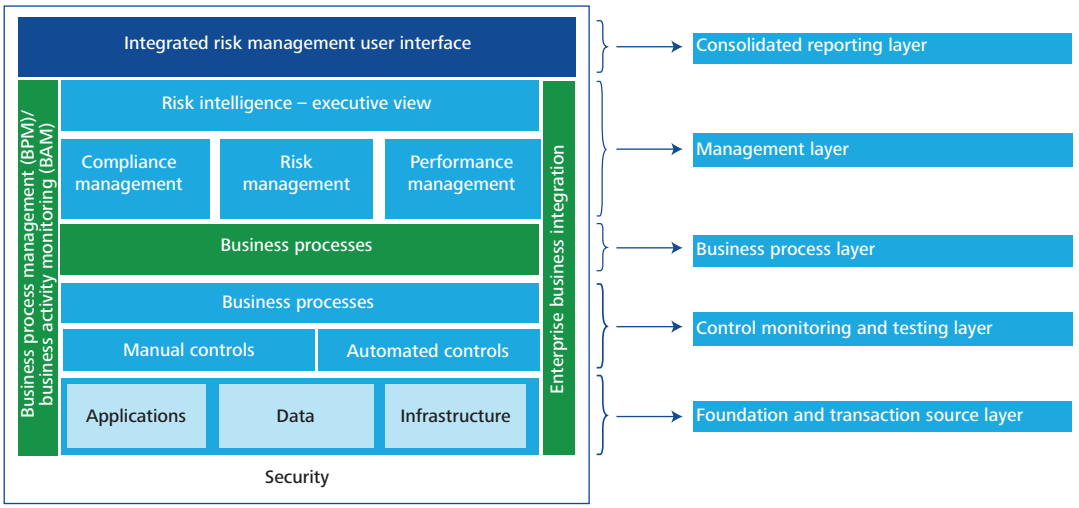
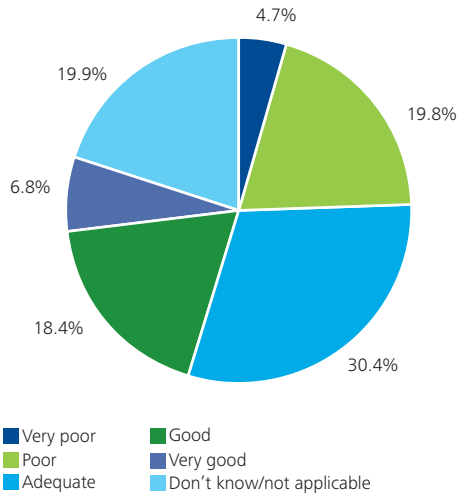


Figure 10. Deloitte executive poll results: Technology
How would you rate your organization's current use of technology infrastructure to support risk management?

Votes received: 1,415



Effective data management is also critical to Risk Intelligent enterprise management. At many companies, important information and data systems are left to reside in separate product or business organizations. The result is often redundant, or even conflicting, data housed in separate data environments. In addition, data can lack sufficient granularity and its quality can be uncertain. Depending on their individual facts and circumstances, many companies may want to consider data quality and integration issues in the following areas:

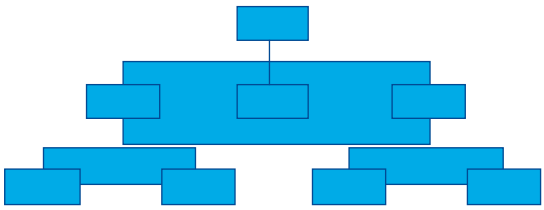
- Customer data and the extent to which it is housed in multiple systems without personally identifiable information
- Legal entity data and the extent to which it is replicated and maintained within multiple systems leveraging incongruous legal entity relationship constructs
- Product codes and the extent to which it is not standardized across systems and defined with distinct hierarchies
- Contract data and the extent to which it is not consistently captured and centrally stored
- Inventory data and the extent to which intensive manual scoring and mapping processes are required and are unable to be reconciled between detailed ledgers and risk reporting systems
- Transaction-level data and the extent to which it is not tied to its requisite summary data, making analysis of anomalies a manual — and sometimes difficult — task

The quality of the data is important in order to enable risk reporting systems to provide senior stakeholders with a high-level holistic dashboard of risk management.

Designing an effective operating model

Model 1: Control/compliance

Figure 11. Control/compliance operating model



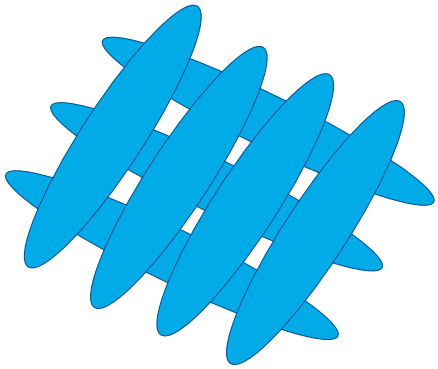
A number of operating models for risk management are possible, each of which has a particular set of benefits and potential drawbacks. We encourage organizations to align their risk management operating model with that of the larger business. In our experience, the greater the congruence between an organization's approach to risk and its overall approach to business, the more smoothly risk management processes operate, and the easier it is for people to learn and execute their risk management responsibilities.

The control/compliance operating model (Figure 11) is hierarchical and emphasizes standardization throughout the organization; a centralized risk management group often assumes ownership and management of particular risks. One advantage of this approach is that it lends itself to the ability to drive alignment among disparate functions and process owners, allowing an organization to more effectively integrate and coordinate cross-functional risk interdependencies and communicate them to the risk group. Conversely, a potential disadvantage is that the risk organization may be perceived as an enforcer of risk policies and rules, leading to a sense of disengagement from risk ownership among the other functions and the business units.

Model 2: Center of Excellence

Generally, we have found that a Center of Excellence model (Figure 12) can help an organization achieve an effective balance between pursuing risks for growth and value creation and mitigating risks for value protection.

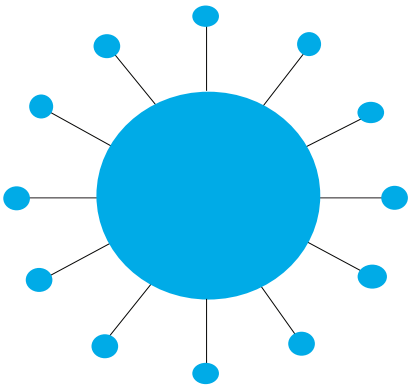
Figure 12. Center of Excellence model



In this type of model, a central group (the Center of Excellence) acts as a centralized resource that provides risk management competencies and tools that can be used across all areas of the enterprise to address a variety of risk issues. One benefit of this model is that the Center of Excellence may be perceived as a business partner whose role is to identify likely or potential critical risks, proactively engage risk owners in addressing risk, build tools and processes, help drive risk-informed decision making, and enhance risk-informed execution. Potential drawbacks of this model include the investment needed to develop tools and processes as well as the fact that the use of the tools and processes are likely to be optional — leaving open the possibility that they may not be fully utilized or adopted by the enterprise's business and risk owners.

Model 3: Reporter/central analysis

Figure 13. Reporter/central analysis model

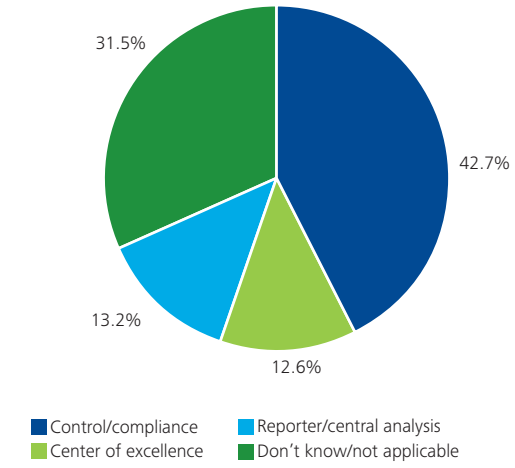


The reporter/central analysis model (Figure 13) is common among holding companies with relatively decentralized operations, and is often used by organizations just starting down the path to Risk Intelligence as their first operating model for risk management. In this model, a central group is charged with identifying trends and reporting on risks across the organization, but each business unit or division maintains its own risk management processes. Risk ownership in each business unit or division rests with line management, which is responsible for gathering risk information and reporting it to the center for analysis. This model is well suited for a holding company in that it avoids excessive disruption to the business. However, it can be difficult for the operating units to perceive the value of the risk organization in a reporter/central analysis model unless care is taken to enable two-way information flow between corporate and the operating units, rather than the operating units simply providing information to the center while receiving no information or guidance in return.

Figure 14. Deloitte executive poll results: Risk operating model

Which risk operating model most closely resembles that of your organization?

Votes received: 1,211



The payoff

It's senior management's responsibility to make the call on which infrastructure investments their organization may urgently need, which can be safely deferred, and which the organization can afford to do without. As you take stock of the options, we encourage you to think broadly about the potential benefits of infrastructure improvements when developing the business case for more effective risk management: greater consistency; higher efficiency; deeper insight into risks and their interdependencies; and enhanced decision-making ability. When all is said and done, an effective common risk management infrastructure is the essential enabler for sustaining a Risk Intelligent enterprise management approach.

Nine fundamental principles of a Risk Intelligence program

1. In a Risk Intelligent Enterprise, a common definition of risk, which addresses both value preservation and value creation, is used consistently throughout the organization.
2. In a Risk Intelligent Enterprise, a common risk framework supported by appropriate standards is used throughout the organization to manage risks.
3. In a Risk Intelligent Enterprise, key roles, responsibilities, and authority relating to risk management are clearly defined and delineated within the organization.
4. In a Risk Intelligent Enterprise, a common risk management infrastructure is used to support the business units and functions in the performance of their risk responsibilities.
5. In a Risk Intelligent Enterprise, governing bodies (e.g., boards, audit committees, etc.) have appropriate transparency and visibility into the organization's risk management practices to discharge their responsibilities.
6. In a Risk Intelligent Enterprise, executive management is charged with primary responsibility for designing, implementing, and maintaining an effective risk program.
7. In a Risk Intelligent Enterprise, business units (departments, agencies, etc.) are responsible for the performance of their business and the management of risks they take within the risk framework established by executive management.
8. In a Risk Intelligent Enterprise, certain functions (e.g., Finance, Legal, Tax, IT, HR, etc.) have a pervasive impact on the business and provide support to the business units as it relates to the organization's risk program.
9. In a Risk Intelligent Enterprise, certain functions (e.g., internal audit, risk management, compliance, etc.) provide objective assurance as well as monitor and report on the effectiveness of an organization's risk program to governing bodies and executive management.

Contact us

To learn more about Deloitte's governance and risk services or to contact one of our global leaders, please visit: www.deloitte.com/risk.