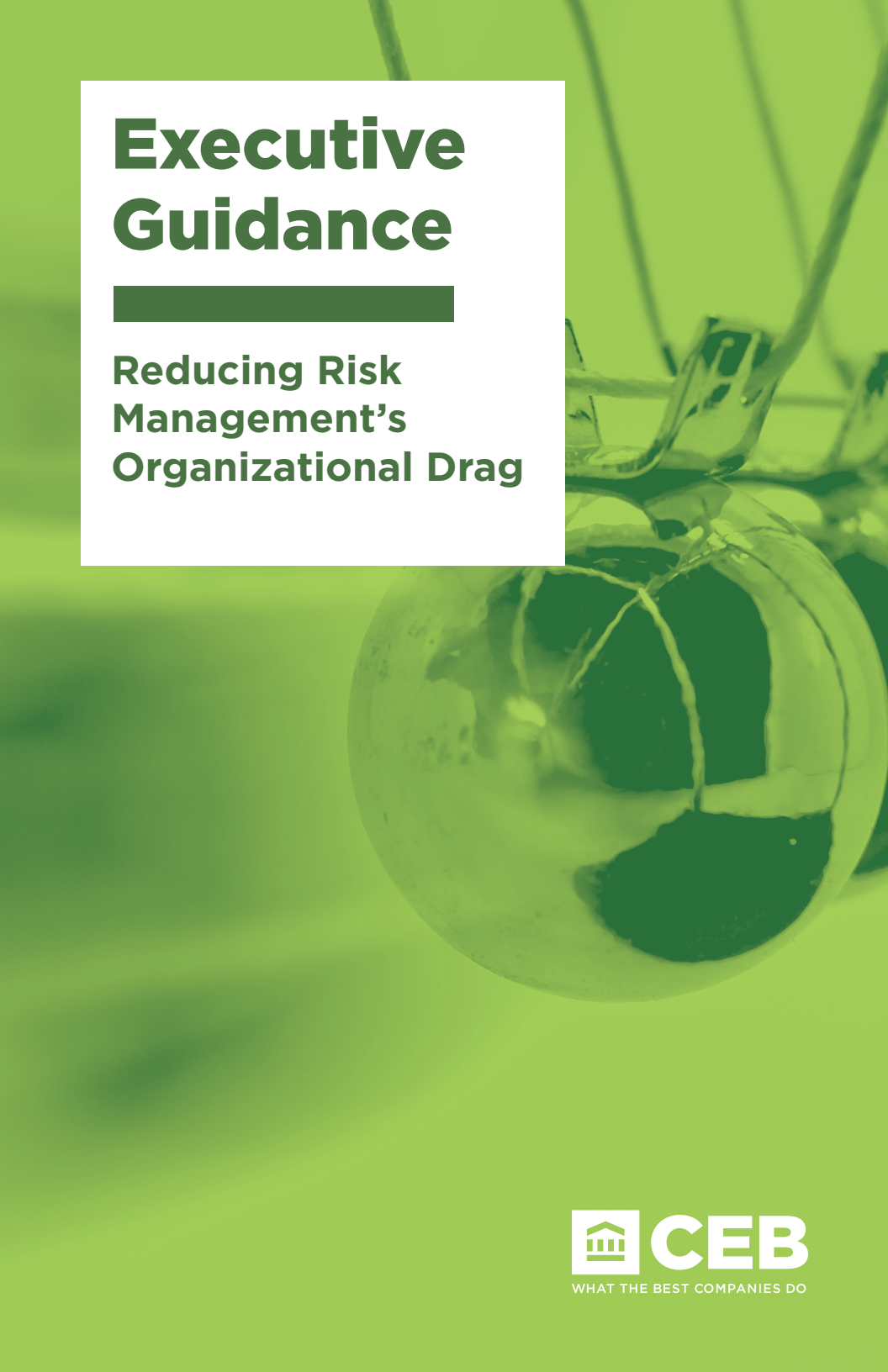


Executive Guidance

A Newton's cradle with several silver spheres hanging from thin wires. One sphere in the foreground is in sharp focus, showing its metallic texture and reflections. The background is a soft, out-of-focus green, matching the overall color scheme of the document.

**Reducing Risk
Management's
Organizational Drag**



CEB

WHAT THE BEST COMPANIES DO

Reducing Risk Management's Organizational Drag

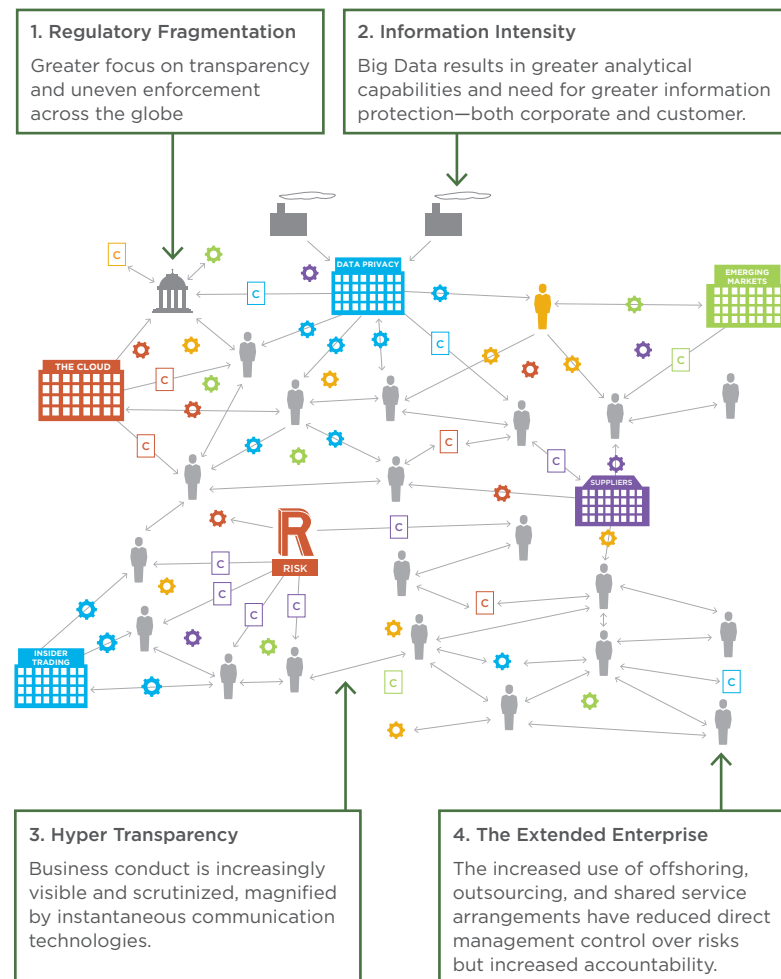
In the early days, risk management was traditionally dominated by financial and hazard risks—predicting or managing against a lack of liquidity or a catastrophic typhoon. In the present day, when those types of risks can be transferred through hedging and insurance, they have taken a backseat to strategic, operational, and reputational risks that assurance functions and business leaders must identify and manage themselves. These business risks, if not managed correctly, can dramatically affect an enterprise's financial results, brand, and even ability to operate—having a severe negative impact on shareholders, customers, and employees.

Rapid change in the risk climate has caused these business risks to grow to new magnitude, immediacy, and effect. Several factors exacerbate the impact of this new risk reality:

- **Regulatory Fragmentation**—Governments and regulators have established more rules to deter risky behavior, but expectations and enforcement are inconsistent from one jurisdiction to another.
- **Information Intensity**—Companies now collect and manage exponentially more data. Although the increased availability of information brings tremendous potential, it poses new risks in cyber security and customer data privacy.
- **Hyper-Transparency**—Instant communication channels such as viral social media amplify and accelerate business conduct's visibility.
- **The Extended Enterprise**—Traditional definitions of third parties (e.g., vendors, suppliers, contractors, agents, resellers) blur as data and processes become highly interconnected.

Risks Are Increasingly Distributed

The Interconnected Risk Landscape



Source: CEB analysis.

With shareholder value as the barometer, the most potentially damaging types of business risks are the strategic ones, such as competitive incursions or declining demand for a core product. CEB's analysis of significant market capitalization declines in the past decade shows that 86% of them were caused by risks that were strategic in nature—with operational risks as a distant second place.

At most companies, however, assurance departments with the formal responsibility of identifying (and sometimes managing) risks—such as with Internal Audit in the following graphic—consider strategic risks to be out of their scope and instead see them as business owners' responsibility.

Strategic Risks Destroy the Greatest Value

Share Price Impact and Audit Time Allocation Across Risk Categories
n = 61.

Likelihood of Occurrence
Percentage of Risk Failure Leading to a Significant Market Decline^a

Executive Time Spent
Percentage of Time Spent by Audit Departments on Risk Types



Source: CEB 2014 Share Shocks Analysis.

^a A significant market decline is defined as a drop in market capitalization of more than 40% in a single year.

It may not be surprising that assurance groups are focused elsewhere—many strategic risks are not “auditable” in the traditional sense. But business leaders are likely not accounting appropriately for strategic risks either. Operational executives know risk and strategy go hand in hand, but they struggle to address them together. Similar to how enterprise risk management (ERM) efforts rarely link cohesively into corporate strategy, typical strategic planning processes run by line executives do not do enough to incorporate and address risks.

To address these new and magnified exposures to all kinds of business risks—and especially to build in formal accountability systems for the most damaging (and elusive) strategic risks—91% of organizations that CEB surveyed are planning to reorganize and reprioritize their risk management approach in the next three years, including bulking up their assurance functions. But these efforts are expensive. CEB research shows that since 2012, compliance budgets are up 10%, information security budgets are up 17%, and ERM budgets are up 22%.

Advising and assisting CEOs, boards, and management teams on this journey is a new generation of risk management consultants and vendors. They promise to help companies adapt their current assurance practices to this new risk reality by establishing processes and investing in new systems. Popular solutions include introducing new sensing and policing mechanisms, updating policies and procedures, integrating risk and governance technologies, and establishing more comprehensive risk reporting (e.g., registers, heat maps)—all largely focused on preventing risk and adverse events.

Although increased investments in risk management and assurance are certainly positive developments, they can have unintended consequences when not implemented correctly. By observing a large number of corporate approaches, we found that an excessive or exclusive focus on risk prevention and formalized risk management processes can create an unintended consequence that CEB and its member executives refer to as “Organizational Drag”—a malady that slows down decision making and execution in organizations, making them less effective.

Three Issues Creating Organizational Drag

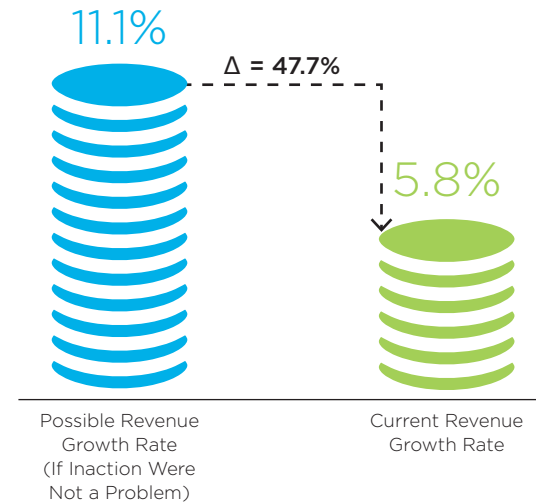
In a decade of research, observation, and work on risk management and assurance with Global 2000 companies, CEB has identified three ways in which risk management activities have gone astray and led to Organizational Drag:

- **Too much focus on risk versus reward can encourage “risk aversion,” resulting in lost growth opportunities.**

Strategic risks are potentially the most damaging to companies, but addressing them in the same way that other risks are managed can be even more damaging. The risk prevention activities (i.e., eliminating any chance of risk) that are appropriate for other kinds of risks can lead to avoidance or aversion of strategic risks that companies would be better off taking. When companies overemphasize the risk (not reward) of strategic decisions such as developing new products, entering new markets, or selecting merger and acquisition targets, they can inadvertently foster indecision or inaction among executives and frontline staff by making them too cautious.

In a CEB survey, 60% of corporate strategists characterized their companies' decision making as slow, particularly for difficult and risky decisions. According to these strategists, slow decision making is the primary impediment to growth—not shortages of capital, funding, or growth opportunities. As you can see in the following chart, executive inaction (defined as the failure to make decisions or act to accelerate growth) costs companies almost half of their potential growth rate—making it one of the most pernicious types of Organizational Drag.

Executive Inaction Costs Companies Revenue Growth
Possible Versus Current Growth Rates in Percentage Terms,
as Cited by Respondents
n = 79 strategy executives.



Source: CEB 2012 Strategy Growth Survey.

This impediment is partially explained by the rise of fear-related biases such as second-guessing, fear of failure, risk aversion, and crisis-mode mentality. These biases have increased significantly in the past three years and can be induced by the perception of too many penalties for taking risks or an improper balance between risk and reward.

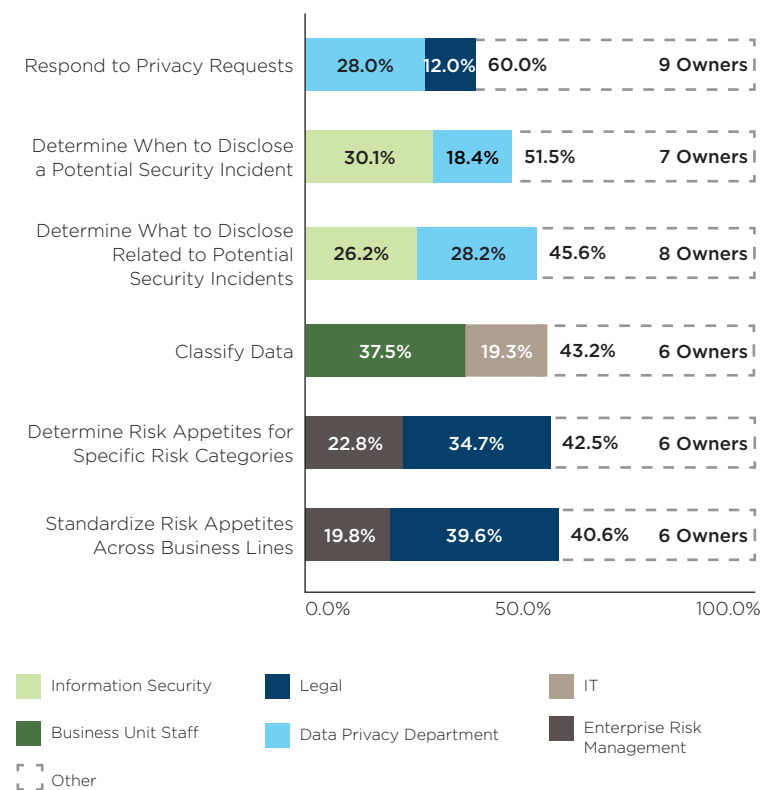
- **By employing their own identification and reporting processes, disparate risk functions are duplicating work.**

Each risk management function in a company—Legal, Compliance, Internal Audit, Cyber Security, Safety, and Quality—focuses on addressing very specific risks. And at many companies, the group and concept meant to unite them all—ERM—is a separate function with its own scope, rather than an umbrella function across risk departments and activities (as it was originally conceived). The net result is confusion not only among assurance groups about who owns what, but also among business leaders who are often forced to coordinate efforts with multiple risk management groups, complete several risk assessments, digest numerous and often contradictory reports, and deal with a lack of prioritization and sequenced risk initiatives. That points to another type of Organizational Drag: significant tax on the business from partnering with all of these groups, which indirectly increases the necessary investment, thereby lowering the ROI from risk management efforts.

This drag is particularly acute in areas such as information risk. As the following chart shows, diffuse ownership hinders organizational agility for risk management and incident response, creates gaps in risk coverage, and distributes responsibility. Ironically, when organizations throw a lot of their best resources at the problem, nobody knows what they are supposed to do or own.

Unclear Ownership Creates Organizational Drag

Percentage of Information Risk Activities “Owned” by Each Function
n = 88 chief audit executives.



Source: CEB 2014 Audit IT Benchmarking Survey.

- **An over-focus on process misses the fact that people are the biggest source of risk and fails to make employees part of the solution.**

Risk management that focuses too much on process and systems—but not enough on enabling better, more proactive risk decision making by employees—overlooks that business risks are magnified or minimized based on human behavior and judgment. Behavior and judgment are highly variable and unpredictable. People make decisions that either create or mitigate risk for the company, choosing to speak up when things go wrong or to behave in ways that solidify or undermine the company's position.

Although many executives know intuitively that human judgment drives risk decisions, they do very little to incorporate it into existing systems, processes, or reports—in effect, taking the most influential variable for granted. Executives scrutinize their processes and trust their employees' judgment—it should be the other way around.

Rather than investing further in process, systems, or reporting, executives must understand how collective judgment impacts critical decisions. Specifically, they should ask themselves the following questions:

- Have our risk-sensing mechanisms that monitor—or our training programs that try to steer—human behavior kept pace with these new risk realities?
- Are the IT or analytics solutions proposed by consultants and vendors doing anything to improve the judgment of our employees, managers, and leaders?

Most companies do not currently spend their risk and compliance training budget where judgment lapses are most likely to occur. They spend the largest amount of training and communications resources on senior leaders, thinking that if they can achieve perfect tone at the top, the trickle-down theory of good behavior will apply. However, CEB research shows that the assumed trickle down is not happening. In fact, most organizations need to worry more about their middle managers and frontline employees than they do their senior leaders. While only 1 in 15 senior leaders poses a high risk, one in seven middle managers and one in eight frontline employees pose a high risk. Although this greater risk among more junior employees is worrisome, of even more concern is that the majority of the staff in these roles do not believe they are receiving risk management training and/or that their direct managers (the firm's leaders) understand or communicate the importance of risk management.

Human Behaviors Impede Effective Risk Management

Survey Results on Employees and Risk



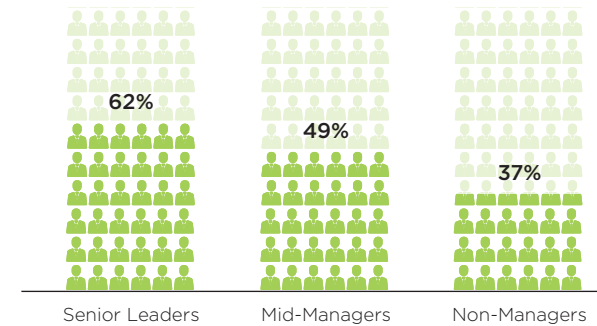
Source: McKinsey & Company, "Flaws in Strategic Decision Making: McKinsey Global Survey Results," January 2009, http://www.mckinsey.com/insights/strategy/flaws_in_strategic_decision_making_mckinsey_global_survey_results; CEB 2013 Audit Survey; CEB analysis.

Risks Are Less Apparent Among Non-Managers

Percentage of Role That Selected "Agree" or "Strongly Agree" on a Seven-Point Scale

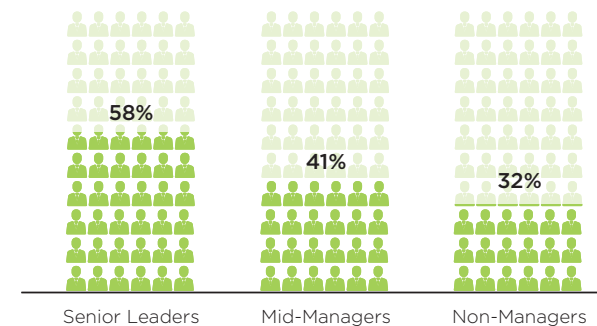
n = 6,473 full-time employees at companies with more than 500 employees.

Q: Do You Understand the Business Risks Inherent in Your Role?



Source: CEB 2013 Global Labor Market Survey.

Q: Do Senior Leaders Communicate the Importance of Risk Management?



Source: CEB 2013 Global Labor Market Survey.

What Risk Leaders Do

The more complex our risk landscape becomes, the harder companies will have to work to focus on strategic risks, clarify risk management responsibilities, and incorporate human judgment and behaviors into their risk lexicon. If the organization's risk management processes are unfocused, unclear, and confusing, employees will make the wrong decisions about risk, creating a drag on the organization's effectiveness. If the leadership team can steer employees toward asking the right questions, making timely decisions, escalating and reporting the correct set of issues, and taking the most appropriate risks, those employees will stop being part of the Organizational Drag problem and instead become part of the solution.

Among the more than 10,000 companies that make up CEB's global membership—including almost 2,000 general counsel, chief compliance executives, chief audit executives, chief information security officers, and heads of ERM—the best companies employ three standout risk management practices to avoid Organizational Drag:

- 1. Incorporate Risk Management in Strategy (and Vice Versa) and Establish a Healthy Risk Appetite**
- 2. Coordinate Disparate Risk Information for Decision Makers**
- 3. Manage Human Behavior as Part of the Risk Management Process**

1. Incorporate Risk Management in Strategy (and Vice Versa) and Establish a Healthy Risk Appetite

Strategy is about both growth and risk; the upside and downside of major business decisions should always be considered equally. But as we have noted, those factors are too often out of balance. Executives need a shared understanding of the firm's willingness to accept and manage risk at all levels—from strategic to operational. Failure to identify and manage strategic risks can be extremely damaging, but hyper-focus on risk over reward can rob companies of important growth opportunities. To avoid either extreme and achieve a happy medium, organizations can do the following:

- **Avoid a prevention approach to strategic risk; instead, guide executives toward appropriate risk taking.**

Tactics used to prevent risks from being taken can exaggerate existing cultures of risk aversion. Most organizations are not open to risk-taking; in fact, only 20% of ERM executives identify their corporate cultures as “risk seeking.”

The word “risk” derives from the early Italian word “risicare,” which means “to dare.” In this sense, risk is a choice rather than a fate. Leading companies view every decision they make as a risk decision; they explicitly link risk to overall corporate strategy and deliberately choose their risks with great calculation. They try to strike a healthy balance between viewing risks as opportunities and using proper risk management as a protection shield, not an action-stopper. In short, leading companies win because they empower their employees to *take* and *manage* risks, not because they do a better job *preventing* them.

- **Align strategy and risk processes whenever possible (and where appropriate).**

Most strategy and risk groups currently have non-synergistic workflows because they run as parallel, siloed processes. To get the most leverage and provide balanced perspectives on important decisions, the strategic planning process should be informed by the annual enterprise risk assessment, or vice versa. In addition, the assumptions related to risks need to be clarified and documented in the strategic planning process itself. Incorporating multiple perspectives on both risk and opportunity removes biases in the planning process and improves confidence in strategic decisions.

Scenario planning is a common approach that incorporates strategy and risk. Leading companies are increasingly conducting scenario analyses on hypothetical strategies to identify potential outcomes, associated risks, and alignment with corporate risk thresholds. Those tactics allow executives to make strategic trade-offs with an informed view of risks and help prioritize strategic initiatives. Assurance functions can help pressure-test assumptions and scan the organization for inconsistencies, but not at the expense of crowding out essential, valuable audit work.

- **Establish a shared company-wide risk appetite.**

Embedding risk in strategic planning, and vice versa, is most effective during planning months and for a short time afterward. But during the rest of the year, risk-comfortable executives who lack clear understanding and guidance on what is, and what is not, an acceptable level of risk will expose the company to greater risks through their day-to-day decisions. And risk-averse executives will favor safe strategies that result in lower growth rates and missed opportunities. The executive leadership team—in concert with strategy and risk functions—can prevent both types of extreme risk behaviors by clarifying the acceptable level of risk and holding decision makers to that standard throughout the year.

The best companies create formal statements of risk appetite, but in doing so avoid overly quantitative frameworks because they do not adequately guide strategic and day-to-day decision making. Instead, they use layman's terms and real world dilemmas when talking about risk appetite, which are more applicable and improve judgment. A simple series of questions can make explicit the decision-making process that many individuals implicitly evaluate in their own minds:

- How comfortable are you with uncertainty?
- What would you be willing to trade off?
- When choosing between two options, would you sacrifice one against another?

In considering these questions, executives and employees attain a shared understanding of risk, which becomes more embedded into day-to-day decision making as opposed to being a discrete, calendar-driven exercise.

Integrating risk assessments into the strategy-setting process and reinforcing a shared risk appetite throughout the leadership team will help companies make more effective risk-based decisions. From our experience, leading companies that ensure a risk-based context for strategic decisions improve decision quality by as much as 42%, and companies that effectively reduce risk aversion can accelerate executive action by 34%.

2. Coordinate Disparate Risk Information for Decision Makers

When presented with a picture of assurance functions at their most siloed extreme (i.e., separate, uncoordinated groups that confront the business with a confusing array of disparate processes and reports), some companies' first impulse is to integrate the functions. But disparate information inputs and outputs are more to blame than the lack of organizational integration—and sometimes integrating organizational charts does not solve the problem of disparate information silos.

Although each risk and assurance function will continue to respond to distinct regulatory mandates—which probably justifies their continued separation—business leaders should demand a more seamless experience. Streamlining the data collection process (inputs) can reduce coordination costs with the business, and integrated analysis and reporting can improve the overall insight value of risk-related reports (outputs). Using a more coordinated approach, with streamlined and properly scaled “asks” of the business, will reduce repetitive burdens and Organizational Drag. Furthermore, CEB does not believe this information integration requires expensive technologies—just a few different decisions. Leading companies expect their assurance functions to use the following tactics to streamline processes:

- **Ask operational managers only for what is really needed—and only ask them once.**

Prioritize, sequence, and integrate the information collection process across multiple assurance and risk functions at your organization. This includes everything from collecting only vital risk information, avoiding duplication of questionnaires and assessments, and—if inputs must be separate—ensuring the data definitions and metrics of separate surveys are consistent and business leaders are not simultaneously receiving multiple requests they perceive to be overlapping.

- **Use existing data assets instead of collecting new ones.**

Leading companies use existing datasets to better predict where risks could occur in the organization, rather than buying or creating new systems and surveys to obtain that intelligence. For example, they use their employee engagement survey results to assess whether engagement levels affect employees' willingness to take risks. A simple survey question such as, “I feel free to take informed risks in getting my work done,” can flag pockets of risk aversion that inhibit innovation. Similarly, a negative response to a statement such as, “I feel comfortable speaking up when I see a potential risk issue,” can indicate potential misconduct is not being reported or addressed properly.

Other useful functional datasets that probably already exist at your organization are detailed in the following graphic.

Functional Datasets Contain Valuable Risk Indicators
Corporate Information Systems and Key Data Fields

	Functional Partners	Compliance Risk-Relevant System	Risk Indicator Examples
	Procurement	Third-party database	Subcontractor due diligence
	Information Technology	Information Security Incident Database	Data privacy breaches
	Human Resources	Human Resources Information System (HRIS)	- Employee “career moments” (e.g., layoffs, role changes, restructuring) - Senior management involvement in noncompliance cases
	Sales and Marketing	CRM database	Customer complaints
	Finance	Accounts Payable	- Improper payments - Travel and entertainment expenses

Source: CEB analysis.

▪ Upgrade critical thinking skills.

Even at companies that have invested in technology engines to better identify risk exposures, assurance functions (particularly junior staff) are not always able to draw and communicate true insight on business risks from them. To help staff better extract insight from risk information, leading companies are building their teams’ critical thinking skills in areas such as data analytics (particularly taking unstructured data and isolating predictive indicators of future risks) and root-cause analysis (e.g., isolating why risk information is not flowing through the organization). Companies must build these skills into training not just for assurance and risk professionals, but for all business managers and employees who will need to coordinate and interact with them in sensing and responding to risks.

▪ Encourage greater information flows—particularly self-reporting—from the middle of the company, not just from senior leaders.

To reduce the constant demands on senior leaders and extract information that often differs from what they get from the senior levels, many assurance leaders are measuring the “mood at the middle” instead of just “tone at the top.” Mid-level managers are an important source of risk information; they receive real-time, candid feedback from employees about potential issues and have the greatest ability to stifle or amplify those issues by how they react and what information they choose to pass on.

3. Manage Human Behavior as Part of the Risk Management Process

To create information pull instead of push, leading companies encourage and reward managers for coming forward with self-identified problems. Management self-reporting of issues uncovers problems that risk defenses may never have detected, and it's great economics: effective self-reporting reduces the need for in-depth audits (both internal or external). If companies can raise management and frontline awareness of key risks such that management can identify issues independently, they can reap benefits such as cost savings and more effective risk mitigation. Leading companies see a 93% drop in outstanding risk and control issues when management self-reports an outstanding risk issue.

Companies' greatest risks are their people. Instead of focusing disproportionately on risk processes, leading management teams and assurance groups anticipate and manage the root cause of most risks: human behavior and judgment. They recognize that behaviors, like any other variable, can be quantified and systematically addressed. In fact, behaviors can serve as an important leverage point for assurance functions and leadership teams. Instead of having to identify and mitigate myriad types of risk, they can focus on a singular root cause—their employees—and use them to solve the problem.

Companies that lead in this area do the following:

- **Screen people—not just processes—for risk indicators.**

The best companies use their employment brand and employee value proposition to showcase their position on risk and related areas (e.g., ethics, quality, safety) and incorporate risk screens into their hiring and talent assessment programs. They explicitly ask questions related to risk tolerance and risk appetite when interviewing and onboarding staff and monitor how those tolerances change as employees' progress through their careers. Leading companies also use exit interviews as a valuable source of risk information. Predictive behavioral analytics that identify the types of personalities and judgment tendencies that lead to risky behavior can help weed out risky behavior, sometimes before it even enters the organization. In addition, time and money spent on upfront talent analytics can reduce both future training and remediation investments. For example, identifying—and not hiring—employees who are more likely to cut corners on safety procedures can ultimately reduce the amount of time and money spent on safety processes and training, not to mention lawsuits and cleanup costs from avoided mishaps.

- **Incorporate human capital risk into risk assessment management dashboards.**

Leading companies feature risk culture and soft controls prominently in their HR, risk, and board reporting and embed it into their ERM processes, audit methodology, and compliance programs. These metrics increasingly provide leading indicators of where risk may arise in the corporation. Conversations with the boards at these leading companies frequently relate to behaviors of at-risk employee population segments and appropriate remediation steps. The metrics they look at address decisions that employees are making, the value at risk of those decisions, and the conditions that allow employees to make better choices.

- **Teach not only rules but also principles that require (and develop) judgment.**

It is accepted wisdom that better employee behavior comes from more awareness and compliance with rules. But companies cannot have rules for every possible risk contingency. Although leading companies establish clear and direct rules for more specific (and nonnegotiable) sources of risk, they also provide principles-based guidance on acceptable risk taking that enables frontline employees to exercise their judgment, as opposed to simply giving them rulebooks that numb decision-making skills. This tiered approach fulfills the requirements of sound compliance and awareness while also preparing employees for decisions that must be made in the inevitable gray areas that policies cannot always explicitly address.

- **Target risk and compliance training at high-risk employee segments.**

Leading companies tailor their communications and training on risk for different employee populations—particularly the ones that carry the most exposure. Using questionnaires that identify employees’ responsibilities for making important decisions or analysis of the job families or departments fraught with the most risk, compliance departments alert the most risk-laden employees to their potential exposure and tailor training to ensure applicability to their more complicated workflows and decisions.

The best companies are also investing in training that promotes employee *application* of key risk and compliance concepts, which is more effective at reducing risk than training designed simply to raise *awareness* of those concepts. In fact, moving from best-in-class awareness (e.g., “Do I know the risk?” “What are the risks?”) to best-in-class application (e.g., “How does the risk manifest in the work I do, and how do I protect against it?”) reduces observed misconduct by 4% and produces a 15% increase in reporting risk-related issues.

Although much of the prevailing thought on risk management focuses on processes, technology, and other quantitative aspects, research shows that investments to explicitly address the human dimensions of risk management have significant payback. Companies that explicitly measure employee behaviors in the hopes of addressing the root causes of risk experience 48% less misconduct.

In part due to an accelerating confluence of new-to-world risk factors, risk management is only going to get more difficult. There is a right way and a wrong way to respond. The best way to implement prudent risk management principles without introducing unnecessary Organizational Drag is to realign the firm's risk appetite with strategy (signaling the proper balance of risk and reward), coordinate risk-reporting processes among various assurance groups, and focus explicitly on managing human behaviors. The ability to manage risks must become an essential leadership competency—on par with (and integral to) executing a strategy, launching a new product, and leading an effective team. Risk management is not a discrete activity for assurance functions to conduct separately from strategy, business processes, and talent management; done properly, it is deeply embedded into all three of those important activities—not slowing them down or adding more cost burden, but actually improving them.

About CEB

CEB, the leading member-based advisory company, equips more than 10,000 organizations around the globe with insights, tools, and actionable solutions to transform enterprise performance. By combining advanced research and analytics with best practices from member companies, CEB helps leaders realize outsized returns by more effectively managing talent, information, customers, and risk. Member companies nearly 90% of the Fortune 500, more than 75% of the Dow Jones Asian Titans, and 85% of the FTSE 100. Learn more at www.cebglobal.com.

Copies and Copyright Statement

The pages herein are the property of CEB. No copyrighted materials of CEB may be reproduced or resold without prior approval. For additional copies of this publication, please contact CEB at +1-866-913-2632, or visit www.executiveboard.com.