Performance-driven risk management
An integrated approach

April 2017
Many innovations that boost the performance and safety of our everyday cars were developed in the high-risk world of auto racing. From the most basic, such as seat belts and rearview mirrors, to the most technical, such as disc brakes and dual overhead cams, these features enable racers to pursue high performance while remaining relatively safe. Finely tuned engines, aerodynamic design and wide tires let drivers push their vehicles to extreme speeds. Safety belts, air bags and fireproof materials let them walk away from accidents should they exceed their limits.

In sports, the arts, science and business, the pursuit of high performance is linked with risk. Pushing limits — or simply reaching beyond a comfort zone — entails risk-taking. High-performing individuals and organizations often take risks that others shun. Yet, when they do, they take risks that make sense for them and for which they are prepared. They recognize emerging risks and respond while they are still manageable. When risk events occur, they have safety mechanisms and risk management capabilities in place.

Achieving high performance in the current business environment demands an understanding of not only risk and risk management, but also truly integrated risk management and how to realize it. As with automotive performance and safety features, risk management capabilities must be integrated if they are to work together toward achieving goals.

Many leadership teams adopt risk management tools or methods without sufficient integration. In Grant Thornton LLP’s 2016 Governance, Risk and Compliance Survey, 43% of respondents noted that their governance, risk management and compliance (GRC) were ad hoc or fragmented and siloed. Only 7% characterized their GRC as value-adding and integrated. The remaining 50% characterized their GRC as integrated (28%) or integrated with some value-added activities (22%).

Findings from Grant Thornton’s 2017 CFO survey provide another window on risk management: 63% of respondents agreed that their organization’s approach to risk management aligns strongly with the business strategy. But a smaller proportion — 54% — agreed that their risk management program is integrated across business functions, which would be necessary to implement risk management aligned with the business strategy. In addition, only 38% judged their organizations as effective at disseminating risk intelligence across departments — a finding that undercuts the notion that risk management is integrated across business functions.

In other words, definitions of integrated risk management vary. That’s understandable because organizations are working to integrate risk management at various levels. Yet, it is senior management’s responsibility to ensure that integration starts at the highest levels — with the value proposition, culture and strategy — so it can then be implemented properly across the business and functions.

Integration usually occurs only at low levels
Much of what is considered integrated risk management occurs at too low a level. Some organizations define it as integration of compliance and risk management or as integration of risk management across business lines. Others define integration as having a chief risk officer (CRO) with responsibility for coordinating risk management activities and reviewing disparate risk reports.

Those can be valid goals, but they do not integrate risk management at a high enough level — with the value proposition, culture and strategy. For example, 64% of respondents to our 2016 GRC survey rated strategic risks as significant, but only 43% rated their measurement and monitoring of those risks as highly effective. When integration occurs only at low levels, risks and related costs remain high and resources are typically misallocated. For example, site-specific risk management tools may be adopted with little coordination with other tools and the overall program; resources may be over allocated to compliance and under allocated to strategic risks; certain risks go unrecognized.

---

Similar situations arise when racing innovations move to production cars. Horsepower exceeds the capabilities of commuters. Ornamental spoilers undermine handling. Carbon fiber mirrors add expense without improving vision. On true high-performance cars, features are integrated into overall design and functionality to work together to assist the driver, pit crew and technicians.

Leadership teams in high-performing organizations accept that risk accompanies the pursuit of growth and profitability. They develop, adopt, deploy and integrate risk management methods that enable performance amid the disruption that now characterizes business. Leadership teams in average organizations are working to catch up to the new reality, while others appear to be floundering.

Following are two examples of risk-taking for high performance in business.

The Apple stores — a positive example
Although they are now among the world’s most successful retail stores in sales per square foot and per employee, Apple stores represented a major gamble back in 2001. They were an untested business model for Apple and could have alienated its existing retailers and sales channels. Most board members initially opposed the idea. The business media pronounced it doomed.

Yet, Steve Jobs was unhappy with the stagnating sales of Apple’s products and wanted more control over the customer experience. His sense of showmanship, design and marketing found expression in the first two stores — opened on the same day in upscale Tysons Corner Center in McLean, Va., and in the Glendale Galleria in Los Angeles County.

While the move was risky, Jobs and his team deemed it worth pursuing because they saw high potential. They realized that while existing retailers provided exposure and revenue, they lacked panache and commitment to Apple products. This put them at odds with the company’s fundamental value proposition, which emphasizes sleek design and enjoyable customer experiences.

iPod music player was poised for launch in 2001, and management realized that the product and the stores could fuel one another’s growth. That assumption proved true, but consider the risks. The stores could fail to attract attention and generate sales. Apple could face embarrassment and lose retailers. But the company might have risked more by continuing with retailers who had their own employees, competing product lines and contradictory agendas.

Apple’s fundamental value proposition had been at risk. So if the stores failed, it would have been a risk worth taking. Management would have placed a bet that did not pay off. But they would not have to say, “We should have had a better design” or “We should have publicized the stores more” or harbor similar regrets. The decision would have been in the range of manageable risks, because the risk was taken to support the value proposition.

This is risk management at the highest level of integration — a risk taken to protect and enhance the value proposition. Apple’s value proposition is to provide an innovative, stylish, superior customer experience. (They don’t talk about computers and devices because that’s not their value proposition.) Apple saw the need to cultivate Apple customers in an Apple environment with Apple-trained employees focused only on Apple products. Given that the company has always wanted end-to-end control of the customer experience, the risks of retail stores were deemed manageable.

Risks to the value proposition can kill the business model, the culture and the business itself, so integrated risk management starts there. This brings us to our second example.
Mortgage lending — a negative example
By now, the lessons of mortgage lending in the 2000s are clear. Misaligned incentives, unsound credit policies and off-loading of risk to third parties, combined with an assumption of ever-rising home prices, led to a mortgage market meltdown and financial crisis.

But that event also underscores the importance of culture. When lenders are making loans without income verification and off-loading hidden risks, they have abandoned basic credit risk management. They have also distorted their value propositions and created an unsustainable culture. Mortgage originators and lenders exist to facilitate loans to homebuyers. If they adopt value propositions based on loan volume divorced from loan quality — welcoming all applicants regardless of ability to pay — they produce a sales culture divorced from a risk culture.

At that point, mortgage lenders must have (or should have) known they were making loans on questionable grounds. They were not managing risk proactively or creating sound risk management and governance cultures. Nor was there any integration of value proposition, culture and risk management.

The resulting crisis led to massive regulatory demands and compliance requirements. This pattern periodically repeats itself in business, as it did with the Sarbanes-Oxley Act, and as it will again. When organizations do not proactively manage risk, problems occur and regulators step in at the behest of stakeholders or injured parties or to save the system.

As these examples show, organizations prosper when risk management is integrated with the value proposition and supports a sound risk culture. This is what we mean by performance-driven risk management. Integration of risk management at high levels enables high performance. Integration at low levels may look like integration while masking risks and inviting disaster.

Risk management versus compliance cultures
Organizations in relatively highly regulated industries often conflate risk management and compliance. However, integrated risk management in a compliance-driven culture is close to impossible. A focus on compliance as risk management causes organizations to place too little emphasis on strategic risks. Respondents to our 2016 GRC study rated compliance risks as the most important (compared with financial, operational and strategic risks), just as they did in the previous three years of the study. They also ranked strategic risks, which can destroy the organization, as the least important in all four years.

In the post-Sarbanes-Oxley Act and post-crisis years, compliance came to dominate risk management in many organizations. Even today, a focus on compliance is understandable. Compliance can be defined through guidelines, promulgated through rules, and enforced through reporting and inspection. Regulators insist on compliance. However, compliance efforts will not in themselves generate sound risk cultures.

Meanwhile, organizations are struggling to integrate risk management — often with little understanding of what that means or why it’s useful. It sounds sensible. Most risk managers — and consultants — view it as integrating compliance and risk management, integrating risk management efforts, or integrating risk management systems. Yet, those approaches don’t start at a high enough conceptual or organizational level, nor do they place compliance in its proper role.
Performance-driven risk management: An integrated approach

5 ways organizations achieve performance-driven risk management
Forward-thinking organizations are recognizing the need to achieve truly integrated, performance-driven risk management, as exhibited in the following activities:

1. Integrating the value proposition and risk culture
Consider all the companies that lost their way when they forgot their value proposition. Minicomputer pioneer Digital Equipment Corporation was founded on making computers smaller, then forgot about doing that and was waylaid by Apple and Compaq. Polaroid invented instant photography, then failed to adapt as technology evolved. U.S. car manufacturers, which pioneered manufacturing efficiency and quality, ignored the process improvement methods of Edwards Deming and other experts, only to see the Japanese auto industry use those methods to outperform U.S. manufacturers in cost and quality.

By the same token, companies that develop and stick with a strong value proposition prosper even as they take risks. Apple is one example. Citicorp is another. In the late 1970s, Citibank placed a major bet on ATMs in New York when the research said it was madness: “Customers want to interact with a teller,” and “People fear being mugged.” But the bank’s goal was to do business with as many households as possible through its nationwide credit card mailings and sprawling branch network. Its value proposition was to make banking easier, so taking a risk on ATMs supported its value proposition — and it worked because customers saw the benefit of 24/7 access to their cash.

Performance-driven takeaway
Organizations with a clear value proposition, and a risk culture that supports it, can achieve higher performance than those lacking either. This is the starting point in aligning risk management with strategy. Even when management takes a risk and fails, the organization will weather the event — provided the risk-taking served the value proposition, risk management was aligned with strategy and risks were proactively managed.

2. Creating true risk management cultures
A risk management culture starts with tone at the top, set by the board in everything from its choice of chief executive to its oversight of risk through the audit committee. A performance-driven risk management culture both supports and addresses risks to the value proposition. The Enron and WorldCom scandals in the early 2000s prompted widespread questioning of the integrity and value of independent audits. The issues were largely cultural and, in response, accounting firms reviewed and reinforced their practices around independence, examination and reporting — and created cultures based more on risk management. Their value proposition was at stake, but the profession and most firms survived as they developed risk management cultures that supported that value proposition.

Performance-driven takeaway
In a sound risk management culture, everyone plays a role in risk management. People do not view risk management as an afterthought or believe it’s solely the risk management function’s job. They understand that their decisions and actions hold opportunities as well as risks for the organization, and they conduct themselves accordingly.
Distinguishing between compliance and risk management

Organizations are recognizing that allowing compliance to drive risk management won’t work. First, risk management enables the strategy; compliance cannot enable the strategy. Second, compliance is about examining and verification, while risk management encompasses decisions and conduct that are often undocumented or difficult to verify. Third, compliance serves the regulatory agenda, while risk management serves the organizational agenda. Finally, regulators can provide guidance only on known risks; meanwhile, organizations face emerging risks, risks specific to their industry or strategy, and risks arising outside regulators’ jurisdictions.

Performance-driven takeaway

Organizations are increasingly viewing compliance as a cost of doing business and treating compliance risk as part of operational risk — one more risk to be managed. Organizations focused mainly on compliance (and loss prevention) define risk and risk management too narrowly. As a result, they find integrated risk management hard to achieve. Performance-driven risk management recognizes the importance of compliance and compliance risk, but addresses them in the context of operational risks within the larger risk management framework.

Integrating cyberrisk into overall risk management

As information and communication technologies become part of every business process, IT risk has morphed into cyberrisk or, more recently, digital risk. The evolving nomenclature reflects the evolution of technological risks. Organizations taking an integrated approach to risk management view cyberrisk as integral to every process, product, relationship, decision and initiative — because it is. The pervasiveness of cyber creates dependencies and vulnerabilities that must be addressed within an approach that integrates cyberrisk management into the overall risk management program. As Gartner Inc., pointed out in a 2016 study, organizations “must recognize the value of integrating these digital components into their overall risk frameworks with a single view of risk for the enterprise.”

Performance-driven takeaway

Cyberrisk management capabilities can either boost or limit an organization’s growth and profitability. Organizations with superior cyberrisk management can develop or adopt new technologies, partner with emerging companies and pursue new solutions more aggressively. These organizations are increasingly looking beyond traditional IT risk management. They are strengthening cyberrisk management by having the chief information security officer or other IT risk manager report to the CRO. They are strengthening cyberrisk governance by including cyber within operational risk, conducting more rigorous cyberthreat reviews and having internal audit provide independent assurance to the board regarding cyberrisk management.

Bringing risk management into real time

Risk events move too quickly for backward-looking approaches to succeed. So a final activity to consider is organizations integrating risk management into operational management practices. This means bringing risk identification, monitoring, assessment, reporting and response into real time. It also means monitoring decisions and transactions in real time, applying predictive analytics to internal and external data and using dashboards, data visualization and other technologies to facilitate real-time reporting. While financial services companies are at the forefront of this trend, leaders in all industries are adopting these approaches.

Performance-driven takeaway

Companies integrating risk management into real-time operations put the related tools in the hands of those who actually manage risk — those in the first line of defense in the businesses and functions — as well as those who advise on and oversee risk in the second and third lines. The more visibility everyone has into risks before or as they arise, the better they can manage risk while pursuing high performance.
Performance-driven risk management: An integrated approach

The pursuit of high performance
These activities mainly characterize the most forward-thinking and high-performing organizations. Yet, those organizations typically lead the way for others. Many of those others have yet to clarify the nature and value of integrated risk management.

A truly integrated approach to risk management creates a context for adopting innovations ranging from appointing a CRO and strengthening internal audit to assessing risks in real time and adopting predictive analytics. Such an approach starts with the organization’s value proposition, culture and strategy, and finds its way into each of the three lines of defense in risk management and governance. Integration of the goals, roles and responsibilities of the three lines of defense must also occur.

As a result of true integration, the organization can pursue high performance by reinforcing its value proposition at the strategic level, protecting and delivering value at the operational level, and managing the full range of risks at every level.

This approach amounts to performance-driven risk management in that it enables the organization to take risks that are worth taking, avoid those that could be devastating and clearly perceive the difference between the two.
About Grant Thornton LLP

Founded in Chicago in 1924, Grant Thornton LLP (Grant Thornton) is the U.S. member firm of Grant Thornton International Ltd, one of the world’s leading organizations of independent audit, tax and advisory firms. Grant Thornton has revenue in excess of $1.6 billion and operates 60 offices with more than 570 partners and more than 8,500 personnel in the United States and at our Shared Services Center in Bangalore, India. Grant Thornton works with a broad range of dynamic publicly and privately held companies, government agencies, financial institutions, and civic and religious organizations.

This content is not intended to answer specific questions or suggest suitability of action in a particular case. For additional information about the issues discussed, contact a Grant Thornton LLP professional.

“Grant Thornton” refers to Grant Thornton LLP, the U.S. member firm of Grant Thornton International Ltd (GTIL), and/or refers to the brand under which the GTIL member firms provide audit, tax and advisory services to their clients, as the context requires. GTIL and each of its member firms are separate legal entities and are not a worldwide partnership. GTIL does not provide services to clients. Services are delivered by the member firms in their respective countries. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another’s acts or omissions. In the United States, visit granthornton.com for details.

© 2017 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd