Enterprise Risk Management: Minimizing Exposure, Fostering Innovation and Accelerating Growth

A systematic examination of risk exposure can help organizations design strategies and implement initiatives to minimize risk, strengthen their brand, and stay in step with new, disruptive technologies.

Executive Summary

Formal processes for enterprise risk management (ERM) have been mainly limited to large companies in highly regulated fields, such as financial services and healthcare. In more technology-focused businesses that center on software development and Internet-based products and services, risk management is often viewed as an obstacle to innovation. That’s because companies in these sectors place a high premium on innovation and developer-friendly environments. The ERM stigma is reinforced in a recent study by the American Institute of Certified Public Accountants (AICPA), which found that only about 25% of organizations that responded claimed to have implemented an enterprise risk management program.¹

The purpose of this white paper is to counter negative perceptions of ERM programs and reinforce the benefits of these initiatives which, when properly implemented and maintained, can lessen risk, accelerate strategic development and bolster bottom-line growth.

We believe that ERM should be approached with the following points in mind:

- Understanding a company’s risk profile is nothing more or less than understanding the environment in which the company exists and functions, which is key to establishing an appropriate product mix that supports revenue growth.
- Knowing an organization’s risk exposures and their potential real-dollar impacts is critical to a sound resource-allocation strategy.
- A first-class ERM program, built upon a formal framework and continuously updated to reflect
circumstances as they occur, is possibly the single most valuable tool a company can have for managing its overall strategy and the allocation of its resources.

• Finally, rather than being regarded as a barrier to innovation, ERM should be viewed as an invaluable asset when transforming a great idea into a successful and profitable product — with less risk over both the short- and long-terms.

**The Importance of Enterprise Risk Management**

Simply stated, the failure to understand your business’s risk profile and take the appropriate steps to mitigate its major exposures will cost money, and directly affect the company’s bottom line in the following areas:

**Project/Product Selection**

Revenues are the lifeblood of business. When allocating resources to projects and product-development efforts, it is crucial to target and analyze areas of risk before taking these actions. Failure to do so amounts to tossing money in the air and hoping it lands on something profitable. Assigning resources without understanding the potential effect on the business can jeopardize a company’s brand and result in a product that could potentially fall flat — either because it doesn’t fit a need or cannot compete with a major (and better resourced) player.

**Market Positioning**

A technology vendor that is not ready to compete in emerging markets (i.e., the Internet of Things space or predictive analytics) could be heading for a fall if competitors have a head start. An ERM program can help organizations understand emerging developments and assign the resources needed to stay in step or one step ahead of the next disruptive technology.

**Capital Availability**

Access to capital is critical when launching and implementing strategic initiatives. Even large, highly profitable businesses often need additional funds to make a big strategic push, enter a new market or build a bigger facility. Yet unlike in past years — say 20 years ago — today’s capital markets are unlikely to part with money to simply support a good idea. Although showing some signs of easing control, financial institutions in general have become far more restrictive in doling out credit since the 2008 global recession. They want proof that a company is controlling its risk wisely, which in turn will reduce the lender’s risk.

**Regulatory Compliance**

According to a study published in the *Journal of Enterprise Risk Management*, regulatory compliance has been rated as a top concern of most executives for three years in a row. New regulations, particularly in the financial and healthcare sectors, are issued frequently. Many of these mandates, such as Sarbanes-Oxley, HIPAA/HITECH, Dodd-Frank and Basel II, not only have requirements for how businesses must conduct their operations, but also for how they should manage risk. Although highly regulated entities are well ahead in adopting structured ERM programs, they often enter into contractual obligations with vendors that may not be as strictly controlled.

For example, healthcare organizations frequently have contracts with medical supply vendors, which are not directly affected by HIPAA/HITECH. However, since the purchasing organization is affected, the contract with the vendor will impose a term of compliance with all regulations, which could potentially impact the purchaser. Litigation can be protracted and expensive; it can disrupt all areas of the business and is a huge risk for companies to manage.

**IT Resilience**

One of the most common risks in business is the lack of a truly resilient IT infrastructure. Major IT outages can sap an organization’s revenue stream (particularly if the company conducts business online). These events can also waste resources...
especially when one considers the amount of non-productive time spent by employees troubleshooting and repairing an existing system rather than putting in hours pushing out a new strategic initiative.

In terms of enterprise risk management, resilience covers three primary areas, defined below:

- **Infrastructure.** Ensuring that critical systems/devices within the IT infrastructure are backed up, have hot-swappable parts, use multiple telecom carriers, have multiple paths through the network, and are using hot failover, for example.

- **Disaster recovery.** Making sure that during a major outage situation, when normal resilience controls fail to prevent the outage, services can continue from a remote site, with minimal time to failover and minimal time to return, and with data integrity maintained during the failover and return processes.

- **Security.** Confirming that the organization’s data, applications, systems and infrastructure are safe from unauthorized intrusions – internal and external.

Another risk to consider has to do with a business’s reputation. For example, in the retail world an increasing number of shoppers choose to buy online when that option is available. If a company’s e-commerce application is not up and running, especially during peak seasons like Christmas and Valentine’s Day, prospective customers will “vote with their feet” and find another vendor that can sell them what they want. In the era of Yelp.com and similar sites that enable consumers to voice opinions on retailers in what amounts to real time, unreliable systems pose a risk that can undermine a company’s brand.

Defining Enterprise Risk Management
Based on the results of an informal straw poll recently conducted among practitioners on LinkedIn by the Institute for Risk Management and the Global ISO 31000 Alliance, very few of the 150 respondents agreed on a simple definition of ERM. We prefer the most direct and most useful meaning:

Enterprise risk management connotes a deep understanding of the “ecosystem” in which a company does business, and the use of that knowledge to allocate finite resources in the most effective way possible to remove obstacles to success as much as possible.

While statistical analysis is a tool practitioners use to help develop an overall risk model for a company, it is not the primary emphasis in ERM initiatives. ERM, like quality management and supply chain analysis, is first and foremost a way of thinking about how a company conducts business.

**ERM in Practice**
When developing an ERM initiative, it is best to take a programmatic approach that involves identifying primary exposures and their potential impact; assessing the probability of those exposures creating events; determining the organization’s risk appetite; prioritizing the weighted exposures, and allocating resources for risk mitigation.

**Identifying Exposures**
Identifying major sources of risk exposure is the key activity in developing a risk-management program. In addition to providing a basis for developing an ERM program, an exposure profile can be extremely helpful when reviewing corporate strategies and determining whether the business’s operating plan is on track.

Risk exposure pertains to every aspect of a company’s business, and identifies the areas in which it may not be operating as effectively as possible. The most common types of risk are explained below. Together, they make up an organization’s risk-exposure profile.
• **Financial.** Exposure to capital markets; extending ROI on existing capital investments; the availability of additional capital for projected strategic initiatives (i.e., credit risk), etc.

• **Economic.** Exposure to currency fluctuations, interest rate changes and governmental monetary policy, for example.

• **Legal and regulatory.** Changes in legislation or attendant regulations affecting the industry in which the organization operates; risk of legal liability in tort or contract, etc.

• **Operations.** Internal systemic risk created or aggravated by management decisions. (Corporate policies’ failure to address new situations; significant unexplained deviations from industry best practices and standards; the lack of an up-to-date business continuity plan, and failure to plan for environmental disasters, etc.).

• **The market.** Threats to an organization’s position in its market. (New competitive products; a major new competitor; company’s failure to exploit new disruptive technologies; lack of access to emerging markets, for example).

• **Technology.** Potentially business-disrupting events caused by failure in some aspect of technology, such as insufficient information security; non-existent, untested or insufficient disaster recovery programs; insufficiently resilient IT infrastructure, etc.

Understanding your organization’s risk exposure means understanding the entirety of your business and the world in which it operates.

**Modeling**

Once the risk profile is developed, the identified exposures are placed into a model to determine the real-dollar impact of a given exposure-related event. This model can be simple or complex, depending on the needs of the organization and the mathematical understanding of the people using the information. A simple model includes the following:

• **Probability of an exposure event.** This can be as simple as high, medium and low, with high (for example) being over 50% likely to occur within the next three years; medium being between 25% and 50% likely to occur within the next three years; and low being less than 25% likely to occur over the next three years. For complex businesses, more rigid statistical modeling can be used to determine within a number of standard deviations the probability of an event occurring, for example.

• **Cost factors.** This refers to both the potential cost of a risk-related event and the real-time cost of mitigating the potential risk from exposure. Generally speaking, organizations must consider the cost of capital and discounted cash flows when determining whether to mitigate a risk now or allow for the potential of a future occurrence.

When completed, the model produces a real-dollar impact figure for each risk identified in the exposure profile, allowing for a clear understanding of the cost of risk to the business.

Once created, the model should be regularly updated to reflect the impact of real-world circumstances as they change. Note: The discount rate used for cash-flow analysis should be adjusted at least yearly.

**Determining Risk Appetite**

After determining the real-dollar impact for the exposure profile, it is incumbent upon management to decide exactly how much risk – in terms of actual dollars – is acceptable when compared with the immediate cost of mitigation.

In simple terms, an organization’s leadership must decide how much potential loss can be tolerated, and whether it is cost-effective to invest in mitigating those losses now or incurring them later. This is an extremely critical step, but one performed by only 33% of respondents in the AICPA poll.

**Setting Priorities**

When budgeting for risk-mitigation activities, corporate initiatives and cost-effectiveness must be weighed. Usually, risk-mitigation initiatives that bring the biggest “bang for the buck” will take priority, which is reasonable. However, it is important to remember to address upcoming strategic initiatives, as well as the business’s overall strategic direction.

For example, if a risk assessment determines that the network infrastructure is based on old...
and/or obsolete equipment but the company intends to migrate to a public cloud environment within one to two years, the initiative should be considered against the cost/benefit of upgrading to new routers and switches. Generally, the risk in any given scenario can and should be tolerated if the expense to mitigate it is greater than the negative business impact that the breach or outage would cause. This is another way ERM informs corporate strategy, and corporate strategy informs ERM.

**Leadership must decide how much potential loss can be tolerated, and whether it is cost-effective to invest in mitigating those losses now or incurring them later.**

Resource Allocation

It is critical to integrate ERM program considerations into the organization's short-to-intermediate-range staffing plan. Not only should programmatic budget funds be included for risk-mitigation activities (equipment, services, etc.); staff resources must also be allocated.

Based on a mitigation project's priorities, leadership must determine how best to assign existing staff to mitigation and non-risk-related activities, and build real-dollar impact models to gauge the cost of potentially adding more staff to risk-mitigation projects. Recruitment/HR should also build these additional resources into global staffing plans.

Building the Risk Management Mindset

Often, the single largest obstacle to successful implementation of an ERM program is the lack of understanding and cooperation by employees, from front-line staff to senior management. It is important to establish a risk-management mindset throughout the organization, at all levels. Management must emphasize that each employee plays a key role in executing the program itself, and supporting the overall corporate strategy and future success of the business.

The following is one proven approach to instilling a risk-management mindset into the business:

- **Assimilate.** Embed ERM and a risk-management mentality into affected business areas by creating a risk-management liaison. RM liaisons are then incorporated into the business units and work in conjunction with business teams to ensure that risk-management goals and priorities are built into product-development and delivery processes.

- **Participate.** Give employees at all levels, with all types of responsibilities, a sense of ownership in the ERM process by developing a sufficiently robust business-continuity plan (BCP). Then ensure that employees from each business area understand their roles in the event of a major outage situation. At least twice-yearly exercises should be run to test the BCP and determine its effectiveness.

- **Educate.** Continually monitor and measure the ERM program against expected results. Reports should be company-wide, in-depth (to inform the model and enable continuous updates) and understandable (to educate the employee base and keep them engaged in the ERM process).

Enterprise Risk Management and Innovation

In many organizations, risk management is viewed as the main obstacle to innovation. The market demands new products, quick delivery and disruptive ideas - now. How can a business with a culture that views ERM as part of its very foundation remain innovative, and deliver groundbreaking products to the marketplace at maximum speed?

It is exactly the contention of this paper that the control, transparency and discipline resulting from integrating an ERM program into an organization’s corporate strategy can help a business send cutting-edge products to market faster and less expensively - with fewer defects, better support and with a more complete understanding of the potential benefits to the business’s current and future financials, as well as its position in the marketplace.

As stated earlier, ERM is no more or less than the understanding of a company's business, the environment in which it operates, and the effect that these factors have on corporate strategy and operations. Organizations with a well-designed ERM program understand which “great ideas”
can translate into a product or service that meets a market need and brings healthy returns. These businesses also appreciate how an innovative new product affects the existing or planned offerings in its product mix. Potential production defects have already been identified and mitigated. Barriers to market entry have been recognized, and a plan is already in place to remove them. Obstacles to success are identified and systematically eliminated.

In the event of product defects or service outages, comprehensive support procedures are in place as an integral part of the product-development process. Management reporting is also established—making it easier to measure product performance and identify and exploit new opportunities.

The ERM team is not the people who say “no” — it is the people who say “here’s how.” A properly designed and executed ERM program is a powerful tool, not only for mitigating risk in an organization’s operations, but also for developing and determining the effectiveness of corporate strategy. An organization with a risk-management mindset engages and educates its employees—from leadership to staff—with the belief that preparation, discipline, transparency, and controls are part and parcel of efficiently delivering a consistently outstanding product. The organization is run in the most cost-effective manner, and is quickly able to respond effectively in the event of a major outage situation.

ERM encompasses the entire span of the business, and provides a more complete understanding of the organization and the environment in which it operates. Finally, a successful ERM program fosters innovation by helping to identify and systematically develop new ideas and, just as important, providing an effective framework for delivering innovations to market.

Looking Forward: Conducting a Gap Analysis
The first step in optimizing your ERM program is to evaluate what is already in place. Questions to resolve include:

- Do we have a formal ERM program that is documented and shared with employees and stakeholders?
- Does our ERM program follow a standards-based framework?
- Are we communicating the benefits of ERM to our teams?

Once your organization has a full understanding of its existing ERM program, it should determine if and where there are gaps that are at odds with best practices in your industry. After gaps are identified, develop a plan to prioritize and mitigate those shortfalls. Documentation is key for educating personnel about ERM, and about how best practices are implemented in your company.

An effective ERM program takes into account the company’s fundamentals, including its risk appetite, major exposures, the potential impact of each exposure and the cost to mitigate. Set ERM priorities in conjunction with business priorities, and let those inform your company’s overall business strategy.

To best foster an environment of innovation, make sure your teams are included in creating and implementing an updated ERM program. Innovators need to understand and feel a sense of ownership in the process, and fully understand its effect on their activities before the plan is implemented.
About the Author

Stuart Roseman is a Senior Manager in Cognizant’s Enterprise Risk and Security Consulting Practice. His practice focuses on enterprise risk management, corporate and IT governance, regulatory compliance, network security and business continuity/disaster recovery – working primarily with clients in highly-regulated industries. He has 25 years of experience in corporate and IT strategy, operations, governance, compliance, and risk management across the public, private and non-profit sectors. Stuart has an MBA from North Carolina State University, a JD from Villanova University School of Law, and a bachelor’s in business administration from Temple University. He is a licensed attorney in the Commonwealth of Pennsylvania. Stuart can be reached at Stuart.Roseman@cognizant.com.

Footnotes


3 The Sarbanes-Oxley Act of 2002 requires a company’s senior management to certify the accuracy of financial reporting statements. This act applies to all publicly traded U.S. corporations.

4 The Health Insurance Portability and Accountability Act of 1996 (HIPAA) created standards for electronic healthcare transaction records. HITECH is a specific provision within HIPAA establishing data privacy requirements for covered healthcare records.

5 The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 created a large number of new regulatory restrictions on banks and other financial institutions as a reaction to the financial crisis of 2008.

6 The Basel Accords II and III established minimum capital requirements for banks and other financial institutions to mitigate risk in the event of a future economic downturn.
