



Strategies for Risk Management

RFG believes the objectives of IT-oriented risk management previously grouped into disaster recovery and business continuity efforts must now encompass all business-related risk areas to align investments properly with exposures. Thus, business and IT executives need to establish standardized, repeatable ways to identify, assess, prioritize, and reduce business, organizational, and technology risks collaboratively and effectively. Essential elements including effective communication, executive support, organizational structure, processes, and trust are necessary foundational elements, and can be fraught with potential pitfalls if planning and coordination are not carefully defined. IT executives should work with business executives to architect a simple yet comprehensive methodology based on the enterprise's ability to address the exposure, business impact, cost, and risk severity in order to identify and appropriately mitigate vulnerabilities.

Business Imperatives:

- Like all important enterprise efforts, risk management requires a concerted marketing and communications program to educate constituents about the importance of the project. The recent and continuing onslaught of government and media scrutiny on topics ranging from accounting practices to data security is helping bring these issues into the spotlight and forcing C-level executives to assume accountability for corporate practices. IT executives should work with C-level and other business executives to adopt or construct a risk portfolio management methodology to evaluate business and IT risks and coalesce the funds, people, processes, and technologies required to address concerns.
- While not all areas of risk are IT-related, IT executives can either serve as change agents for risk assessment, mitigation, process management, and tracking, or act in important supporting roles. IT executives should participate in enterprise risk management because of IT's ability to enable and catalyze the required change in many industries, as well as affect and support many aspects of risk mitigation across the business. Additionally, members from the audit, business unit, C-level executive team, finance, legal, and public relations groups should also participate on the risk oversight committee. IT executives and other oversight committee participants should work to align corporate goals, priorities, requirements, and risk aversion levels with the exposures and exposure mitigation solutions.
- Once areas of risk are identified, corporations should employ a risk portfolio management framework to assess exposure levels, business impacts, cost requirements, and resolution priority and importance. It is likely that opinions about components will differ dramatically based on individuals' agendas, backgrounds, roles, etc., which could result in delayed work efforts, improper task prioritization, and misspent funding. Therefore, it is critical that oversight committee constituents agree on the system used for gauging the costs and benefits of each candidate initiative. IT and business executives should adopt a simple, yet effective, risk portfolio management framework that examines the ability to change or manage risk, business importance, linkages to other systems and processes, and potential impact in order to prioritize activities properly.

Risk is an ever-increasing concern receiving a great deal of scrutiny from board members, executives, governing bodies, the media, and shareholders. Whether the topic is accounting practice compliance, data privacy or other security concerns, growing parts of the business in developing nations, offshore outsourcing, past improprieties, or virtually anything else, all business activities carry some degree of risk. As a result, those internal and external forces that are discovering flaws and/or gaps in current operations present a challenge to IT and other business executives. Many different factors bring ongoing scrutiny to these topics, including activities with business partners and outsourcers, the rising number of services being stored on and accessed through public networks, and various prying eyes. (See the RFG Research Note "[The Importance of Mitigating IT Risk.](#)")



Big unknowns are also of great concern. Governments love mandates such as the [Gramm-Leach-Bliley Act](#) (GLBA), Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes-Oxley Act of 2002 (SOX). Corporations can expect many more of these types of laws to appear from federal and state agencies over the next decade, and while they may serve to protect the rights of private citizens, they offer little, if any, guidance for enterprise compliance. For instance, the [Securities and Exchange Commission](#) (SEC) has increased its auditor staff in excess of 27 percent and collected more than \$3 billion in penalties. This is undoubtedly just the tip of the iceberg.

Also, the laws are intentionally ambiguous, forcing interpretations to be argued in lengthy and costly legal battles. Corporate executives will be called upon publicly to account for their management best practices and demonstrate how best efforts were employed to mitigate risk. Therefore, it is incumbent upon executives to have comprehensive knowledge of exposure points and devise incentives, marketing campaigns, and strategies within the corporation and key business partners, in addition, to abate problem areas. Furthermore, a variety of other organizations, including the [Object Management Group](#) (OMG), are working to develop standards for IT compliance to mitigate risk.

Effective risk mitigation requires close internal evaluation of all aspects and lines of the business, and involves changes in people, process, and technology. Numerous companies are recognizing the need to appraise operations and adopt new methods to abandon, fill, or shift risk, but others are still slow to embrace the needed change. This aversion is caused by factors ranging from how deep and wide a review should span, to lack of funding, inability to manage change, and identification of which business units and employees should have task responsibility. None of these problem areas will slow down or prevent liability for failing to address any of the looming problems. Consequently, C-level and other executives must work together quickly and collaboratively to break down any of the existing barriers. Cross-functional teams work well in this complex environment. Therefore, participants from audit, business unit, C-level executive team, finance, legal, and public relations groups should participate in a risk oversight committee and structure a framework for assessing and managing change. (See the RFG Research Note "[Are Cross-Functional Teams \(CFTs\) Really Functional?](#)")

Business units do not exist in a vacuum and, therefore, all are affected, constrained, and incented/disincented by each other and a cross-section of business and operational criteria. At least one member from each business department should participate on the oversight committee, helping to ensure that the requirements and interdependencies at play among business lines are appropriately pinpointed and considered. The charter of the oversight committee should be to identify areas of exposure and their interdependencies, establish criteria to evaluate risk levels, and work to manage required change. Evaluating risk levels and deciding on the order in which vulnerabilities are addressed can be challenging because of differing backgrounds, business objectives, funding allocations, incentives, motivations, and perspectives.

Risk levels should be prioritized based on importance, ability to be affected, and the degree to which change will concretely improve the business. Simply put, this could also be viewed as risk impact dollars multiplied by the cost of the risk's occurrence. Gaining consensus here can be challenging, as each of these areas is highly subject to interpretation. Enacting a concrete risk portfolio management methodology to prioritize tasks and strategically organize mitigation efforts is a key element in successful exposure reduction. The construction of this framework will be discussed in greater detail later in this Research Note. Additionally, part of this challenge should be answered by having some, if not all, of the funding required addressing risk mitigation specifically designated and allocated as such by the business's senior executives. Furthermore, this act unequivocally demonstrates executive-level support for risk mitigation,



which is an essential element for marketing, gaining backing for the group's mission, making external constituents aware of the effort, and building trust.

Universal acknowledgment of, and support for, risk mitigation is the first step required in building the framework necessary to drive change. Since risk mitigation cuts across the entire enterprise and requires collaborative discussion, effort, and funding, highly visible executive support is necessary. Executives at most firms are placing risk mitigation projects at the top of their corporate priorities in order to satisfy stakeholder concerns and to prevent their own forced departures. While some executives simply view risk mitigation as a cost of business, or a Risk, Compliance, and Security (RCS) tax, not all do. The costs associated and value derived from mitigation projects can be off-putting because rewards are not easy to project at the outset. Moreover, large, publicly-traded firms are under constant observation by a myriad of stakeholders and are thus expected to show positive returns on investment in all undertaken activities.

At RFG's thought-leadership Summit series entitled "Reducing Risk, Restoring Trust: A Leadership Role for IT" held in San Francisco on Oct. 27th and 28th, participants shared a few appropriate quotations. One was that "Enron math no longer works," referring to the fact that organizations will need to comply with both the letter and the spirit of [Financial Accounting Standards Board](#) (FASB) accounting. Another is that "Risk is proportional to distance from headquarters or the control point." This poignant quotation lends accurate insight about where executives should diligently invest energy in looking for risk, as some of the greatest exposures may be the most hidden from sight. One quote was a twist on an old maxim: "ROI means reduce odds of incarceration."

As true as that statement may be, the risk management oversight committee should nevertheless evaluate potential projects so as to maximize and quantify the value of where funds are spent. In addition, one of the troubling quotations was one that addresses one of the major flaws in all directives, policies, and processes: "Culture eats process for lunch." To address that issue, one needs to employ the following quote: "Trust, but verify." This clearly defines the requirement that management has in ensuring that its policies are adhered to effectively. (See the RFG Research Note "[Risk Management: Conference Report](#).")

Despite the importance of risk management, no firm can afford to spend an unlimited amount on risk mitigation efforts. There are more risks to be hedged than dollars available and, therefore, risk management plans need to be able to address exposures effectively and economically, while also providing a clear explanation of why other risks are not being addressed at a particular point in time. This phenomenon or strategy is somewhat akin to being naked in the forest, finding a few scarce fig leaves, and then discriminatingly selecting where to put those fig leaves. RFG believes that the best way to prioritize projects is to build Value Chain maps to eliminate any leaps of faith for business and technical processes. This exercise will help to identify organizational resource gaps as well.

The Value Chain map is a simple tool, but very powerful in its ability to divide enterprise processes into their distinct elements by breaking them down into their supporting organizational, procedural, and technological components. Although the process itself is not complex, deriving risk assessment values may be. Stakeholders must evaluate multiple exposure factors.



Value Chain Mapping Exposure Identification Questions

- Where are the exposures?
- What is the severity of those risks?
- To what degree can those vulnerabilities be positively influenced?
- How can the culture be changed in a fashion that does not leave people feeling more at risk? (i.e., "What is in it for me?" "What is at risk for me?")
- What will it cost either to reduce or eliminate the risk?
- What is the worst that can happen if the risk is not addressed?

Source: Robert Frances Group

RFG believes effective risk management requires input from all aspects of the business and top-down, proactive support from executives. Identifying and assessing risk levels can be a daunting task due to the unique agendas and perspectives; thus, business executives need to collaborate in order to construct an unbiased portfolio management framework that can be easily implemented throughout the corporation. Since the capital will not be available to address every exposure simultaneously, lower priority risks will have to be dealt with at a later date. Therefore, it is critical that the risk oversight committee be comprised of constituents from all business areas working together to prioritize projects accurately in order that the dollars spent are allocated to those risks demanding the greatest need for mitigation. IT executives can help play a critical role in the risk management process by helping to identify, enable, and speed the delivery of risk management techniques using automated management and tracking tools in order to validate and verify the success of exposure reduction efforts.

RFG analyst Adam Braunstein wrote this Research Note. Interested readers should contact RFG Client Services to arrange further discussion or an interview with Mr. Braunstein.