RSA

WHITE PAPER

The 10+1 Guiding Principles of Business Risk Management

At a fundamental level, understanding risk is essential for running a business, since optimal business execution ultimately involves decisions that maximize rewards while minimizing the impacts of negative events. Understanding risk enables organizations to best allocate their resources (time, money, etc.) to reduce unacceptable risk, diminish unpredictability and achieve their business objectives.

Certain tenets should guide an organization's strategy for business risk management. These guiding principles should be the foundation for the overall risk management strategy and be part of the fabric of the governance program. A business risk management strategy is not a one-time effort; it often requires a cultural shift in how an organization conducts business. Organization-wide commitment to a paradigm of good governance is critical to the success of a business risk management program. Without such a commitment, the program will be undermined and likely to fail.

The 10+1 Principles

In addition to committing to a strong governance paradigm, the following principles must be ingrained into an organization's business risk management strategy.

- **Ownership**. Organizations need to hold individuals responsible for fulfilling the roles for which they have been employed. The management of risk and compliance activities is everyone's responsibility. This includes not only establishing executive roles but also clearly defining and enforcing responsibilities across all three lines of defense.[1] The three lines of defense (LoD) model characterizes the "people component" of an organization into the three primary functions of an optimized risk management program:
  - **1st LoD—Business unit and operating managers**. These management functions are responsible for the ownership of risks and control procedures within their functions. This responsibility means identifying, understanding and managing their risks as well as ensuring that appropriate controls to manage risk are designed and operating effectively.
  - **2nd LoD—Risk management and compliance oversight functions** (such as enterprise risk, operational risk, security and corporate compliance). Those engaged in this oversight are responsible for the risk management framework, training and challenges to 1st LoD risk assessments.

- **3rd LoD—Independent assurance functions** (such as internal and external auditors). The 3rd LoD is responsible for independently evaluating and reporting on the design and effectiveness of the organization's overall risk management program.
- **Collaboration**. Organizations need to reinforce collaboration across the enterprise on matters of risk and compliance management without regard to organizational boundaries. Collaboration introduces diversity in problem-solving through information sharing, analytics and tracking the right metrics to make the right decisions at the right time.
- **Efficiency**. Automated processes should be designed to drive efficiencies by taking spreadsheets, email, file sharing and manual processes out of the equation and by employing workflows to automate processes. Automation should ensure that the right people are engaged to contribute information and make decisions, at the right time, with the right information, based on business requirements and best practices.
- **Business Context**. A business risk management strategy should promote business context, as informed business decisions can be made only by considering problems within their complete context. Business context means understanding interrelationships in areas such as business hierarchy, stakeholders, business objectives, products and services, business processes, assets, risks, control procedures, policies and procedures, authoritative requirements, and outstanding issues.
- **Positive Assurance**. At the end of the day, good business risk management should derive demonstrable assurance to the executives, shareholders, employees and applicable regulatory bodies. Risk and compliance efforts should focus on "what keeps people awake at night" as well as the many threats that could hinder the organization from achieving its objectives, providing clear evidence of the effectiveness of management's oversight of risk and compliance objectives.
- **Sustainability**. Business risk management requires a persistent commitment to sustain the effort and achieve the strategic benefits. This has to be factored in when designing a program. For instance, while the effort to comply with an individual regulation may be at an acceptable level right now, the processes impacted by that regulation have a tendency to evolve and can quickly grow outside their original boundaries or intent. Business risk management must acknowledge this change and be considered a long-term venture.
- **Consistency**. One can think of business risk management as a big playbook the organization uses to manage risk and compliance issues. The program involves many different processes—from overarching enterprise processes to daily operational processes. The architecture should bring order to this large effort and get employees on the same page with a common framework and strategy.
- **Proficiency**. Business risk management should invoke the concepts of continuous improvement and elimination of redundant efforts. Adjustments of processes to meet multiple goals can result in significant efficiency gains—generally more than initially estimated. In addition, the implementation and evolution of business risk management should strive to simplify complex processes. This means revising complex internal workflows in favor of streamlined and agile processes while retaining appropriate stakeholder governance.

- **Agility.** Given most organizations are in a constant state of motion, the business risk management program must enable agile processes to react, respond to and address changes to the business. Regulatory changes, new business opportunities, technology shifts, reorganized business processes and other factors will constantly barrage an organization, and the risk and compliance implications must be managed in a manner that permits the business to consume, adjust to and manage these changes.
- **Transparency**. The concept of transparency should permeate the business risk management program. Transparency means delivering the right information to the right stakeholders within timeframes necessary for the purposes of enabling effective governance, informing business analysis and providing diverse organizations with information that can be leveraged. This transparency extends to both internal and external stakeholders and includes overall visibility into the structure of the program and the activities documented and managed within the program (such as the status of strategies and objectives, business entities, business processes, risks, controls and compliance with internal and external obligations). It is through the transparency of the business risk management program that positive assurance of its effectiveness is demonstrated.
- **Balanced Effort and Reward**. Finally, the business risk management program should be an effort to achieve long-term balance between the rewards of embarking on the journey and the costs associated with the journey. Organizations need to be smart and calculated in how and to what extent business risk management activities are implemented. Organizations should be thoughtful about the cost vs. benefit of each incremental step in the execution of a business risk management strategy. A keen eye should be focused on the scope and context of the organization's desired governance end-state when preparing the journey to that state. This will help keep your organization from making missteps and pursuing activities that will ultimately slow its progress to the desired end-state.

  Your business risk management program should add strategic value to the organization—enabling the business to focus on strategic objectives and optimize performance, not just simply meet compliance requirements. Ultimately, business risk management is about making decisions—decisions to manage, accept, transfer or avoid risk. These principles should guide the governance, risk and compliance (GRC) and security functions towards a sustainable program that evolves and adapts with the organization.

  Learn more about RSA Archer® solutions for business risk management at rsa.com/grc.

[1] The origin of the three lines of defense concept is not altogether clear, but it is likely an outgrowth of The 1992 COSO Internal Control—Integrated Framework. It explicitly appears in the COSO Enterprise Risk Management draft exposure as the "lines of accountability model." In January 2013, the Institute of Internal Auditors published a position paper effectively endorsing the three lines of defense concept as a best practice in risk management and control. Financial services organizations have long been exposed to the three lines of defense model via the Principles for the Sound Management of Operational Risk.