5 TIPS TO IGNITE YOUR BUSINESS RISK MANAGEMENT PROGRAM

BUSINESS-DRIVEN SECURITY™
Effectively managing risk is critical for the success of every organization. In fact, understanding which risks are worth taking is one of the most important facets of business today. Avoiding certain risks is smart business. But playing it too safe is a sure way to let the competition outpace you. Unfortunately, the complexity of business, the speed at which new risks emerge, and the volatility of risk are all dramatically increasing. This makes it very difficult for organizations to adequately prepare for or respond to risk. In addition, many risks that organizations must contend with, such as information security, are so complex and technical in nature that it is difficult for the organization’s leadership to get the necessary balanced insight into risk across the organization.

This dilemma introduces the real problem—that some critical risks may remain unknown or misunderstood. Without an understanding of risk, human and capital resources may be insufficient or misallocated, and risk may not be managed in a timely enough manner to best stem the risk’s impact to the organization. Business risk management principles provide the means to resolve these issues and increase the likelihood for an organization to achieve its strategic objectives.

With this broad and complex challenge, it is imperative to lay a strong foundation. These five tips will help you in igniting your business risk management program.
TAKE COMMAND OF OUTSTANDING ISSUES

Every organization has issues to address, whether it’s determining the steps needed to achieve business objectives, corrective issues identified by management, or findings that originated from compliance examinations, internal audits, or consultants and regulators. Regardless of the source, it is critical for these issues to be captured, prioritized, assigned to individuals to address, and monitored to ensure resolutions.

Surprisingly, many organizations do not compile and maintain a list of issues they need to address. In cases where they do have a list of issues, they have not established clear accountability for resolving each issue or firm dates by which a resolution will be complete.

Effective issues management is a vital first step in good governance, and requires proactive ongoing monitoring.

By implementing an issues management process, management leaders can see which issues are most important and need to be addressed first. They can make well-informed decisions about the allocation of resources to address problems, and they can actively monitor issues, enforcing accountability to named individuals to complete tasks as quickly as possible to remedy problems.

“See which issues are most important and need to be addressed first.”

90% of organizations do not consider their incident response to be highly effective.
An organization’s objectives may include financial goals, the health and safety of employees, information security, resiliency, environmental stewardship, or a myriad of others. They strive to manage factors that will help in meeting those objectives. Risk represents “the deviation from the organization’s expected objective” (positive and/or negative), and risk management represents the coordinated activities to direct and control risk to the organization. In simple terms, risk management is necessary to increase the likelihood that the organization will achieve its desired objectives.

Capturing, assessing, and assigning individual accountability for managing the organization’s risks is essential for effective business risk management. This helps the organization establish a framework for talking about different kinds of risk in terms that management understands. No longer will technical specialists, such as information security teams, go unheard or misunderstood in the discussion of risk and its potential impact on the organization. They can effectively articulate the problems they see in terms that business leaders understand.

By cataloging risks across the enterprise, the organization breaks down silos, creating collaboration that aligns risk management efforts to best achieve the organization’s objectives. This creates a culture where every manager is a risk manager and ownership of risk is part of each manager’s day-to-day responsibilities, rather than a manager only responding as losses and adverse incidents arise. This culture enables organizations to take on more opportunities and their associated risks because they are better able to manage it.
The old adage still holds true: You can't manage what you don't measure. Without measuring, there is no way to know which activities are significant enough to manage, nor can you assess whether you are making progress in managing those activities. Assessments do not need to be complicated and time-consuming to be effective. For organizations that are starting to get serious about business risk management, quick business impact-oriented assessments are an excellent starting point and well worth the effort.

Business impact-oriented assessments provide management with quick qualitative assessments to prioritize the criticality of business processes throughout the organization. This prioritization affords management an understanding of where to allocate human and capital resources to manage risk and compliance obligations. Periodic reassessment provides additional clarity for the effectiveness of ongoing business risk management initiatives.

73% of senior executives and board members indicate that risks to their companies are increasing.  

Business impact analysis, in the broadest sense, is designed to help determine the criticality of the organization's business processes. This is not just in terms of maintaining ongoing operations, but also understanding what type and how much risk arises from each operating activity. This helps prioritize management resources for the most important processes and creates management efficiencies. This information can also be shared with teams that rely on it the most, including business continuity, information security, operational risk management, and internal audit teams.
ADDRESS INHERITED RISK

Organizations broadly rely on third parties for everything from “white labeled” products and services to window washing, and just about everything in between. In most cases, it is impractical, if not impossible, for an organization to distance itself from risks that could be introduced via a third-party relationship. These inherited risks can present the same likelihood and degree of impact to the organization as if the organization retained the outsourced activity internally.

Consequently, inherited risk can materialize across every type of risk, including information security breaches, regulatory compliance misses, resiliency and supply chain interruption, operational errors and fraud, and reputational damage, to name a few. In some cases, inherited risk can be material and could result in significant losses for the organization, widespread negative publicity, and even put the organization out of business.

The starting point in addressing inherited risk is to capture a list or catalog of third parties that introduce significant inherited risk to the organization. For organizations that are unable to do this today, they will be caught off guard when something goes wrong due to a third party. Maintaining a list of third parties and assigning each third party to a manager reinforces that managers are responsible for understanding and managing inherited risk.

Maintaining a list or catalog of third-party relationships, assessing the type and amount of inherent inherited risk, and assigning third parties to manage this risk helps the organization identify material third-party relationships. Informed decisions can be made to allocate scarce resources to manage high-risk relationships, and contingency plans can be created, if necessary, to stem the risk to the organization if the third party fails to fulfill its obligations.

THIRD PARTIES continue to be the single biggest worry for compliance professionals.
EXPLOIT THE FOUNDATIONS

With the building blocks of business risk management in place, the organization is in an excellent position to build upon them to gain even greater efficiencies and effectiveness across all of its governance programs.

Companies that are able to link business risks with their strategic imperatives are more likely to have achieved an annual profit margin of greater than 10% over the past three years, as well as better profit margin growth.\(^2\)

WHAT WAS YOUR COMPANY’S AVERAGE ANNUAL PROFIT MARGIN OVER THE PAST THREE YEARS?

RISK LEADERS

ALL OTHERS

Companies that are able to link business risks with their strategic imperatives are more likely to have achieved an annual profit margin of greater than 10% over the past three years, as well as better profit margin growth.\(^2\)
Each one of the foundation elements sets the stage for building a broader and more mature business risk management program.

1. Managing issues properly can lead to improved compliance processes. Identifying regulatory obligations and documenting policies and procedures tied to issues can increase awareness of established obligations. It can also provide evidence of how the organization operates relative to policies, procedures, and regulatory obligations.

2. With a risk catalog as the starting point, the program can be expanded to encompass a broader operational or enterprise risk management perspective. The organization is in a position to understand the plethora of risks it faces, including errors and fraud associated with people, processes, and technology, that could impede the achievement of objectives. The organization can capture risk mitigation and transfer strategies, understand which controls are working, and which controls need to be fixed or abandoned if they are unnecessary or overly expensive relative to the risk.

3. By incorporating a documented IT infrastructure within the business impact analysis framework, the organization is in a much better position to enable business-driven security and enhance its business continuity management program.

4. A third-party catalog provides the groundwork to index external parties and manage contracts, risks, and service-level metrics.

5. Lastly, by placing an audit solution around your program, auditors can more effectively evaluate management’s internal control framework, respond to problems more quickly, and collaborate with management more closely as organizational changes occur and issues arise.
CONCLUSION

Business risk management helps organizations define and enforce risk ownership through accountability; cross business lines and organizational boundaries to collaborate, consolidate data, and enable risk analytics and visibility; and automate processes for greater efficiencies. By implementing business risk management, your organization can take command of risk to proactively prioritize and address the risks that matter most, and evolve your risk management program from top to bottom. Moving your program from one that only affords pure protection to a strategic enabler of the business.

To learn how the RSA Archer Suite of business risk management solutions can enable you to ignite your business risk management program, visit RSA.COM/GRC

SOURCES: