How to achieve excellent enterprise risk management

Why risk assessments fail

The usual suspects

- Lack of alignment with strategy and business activities.
- Inadequate planning and communication.
- Misconception of time commitment required of business and functional participants.
- A focus on current or past risks rather than the future.
- Generic rather than company tailored risk inventory structure and negative risk definitions.
- Mismatch between assessment complexity and risk complexity.
- Lack of defined perspective and duration which leads to inconsistent assessment responses.
- Failure to validate identified key risks with executive management ("C" Suite).
- Ineffective or non- existent risk prioritization criteria and methods.
- Creation of unmanageable risk list vs "top 10" risk profile.
- Reporting content and design.
- Incomplete or lack of comprehensive risk plans.
- Excessive time from initial identification and prioritization to action plan development results in "stale" risk list.
- Lack of integration into business decisions.
- Viewing the risk assessment or assignment of a risk plan as the end of the risk management process.

Overview

Risk assessments are a common tool for understanding business issues and potential consequences from uncertainties. Unfortunately, risk assessments are often informal, poorly constructed and fail to identify and prioritize key risks impacting strategic and business initiatives' outcomes. The sources of risk assessment failures range from poor communication, design, execution and content to inconsistent participation and interpretation.

We believe that a disciplined, continuous and business outcome focused risk assessment approach that moves beyond the traditional annual "heat map" exercise can greatly improve success and directly support both strategic and risk assessment objectives and goals.

This article identifies the primary reasons for risk assessment fatigue and failure, and ways to improve success. Risk assessments are a foundational element within a risk management program, but often fail to fully support both program and business objective.

The communications challenge

Defining risk is critically important to setting the right tone in risk management communications. Discussions of risk and risk management do not need to be negative. Risks are natural outcomes from business activity. Risks are simply uncertainties— and can have both negative and positive outcomes.

pwc

Discussions should focus on thoroughly understanding risks and the organization's capabilities to manage those risks. Organizations can take on more risk if those organizations decrease the likelihood of negative outcomes or improve the likelihood of positive outcomes. When viewed in that context, risk management is an enabler to the achievement of strategic objectives.

Failures in the risk assessment process are often related to poor communication both in expectations setting and in the development, understanding and usage of risk management information. A plan should be developed to carefully craft the key messages before, during and after the risk assessment. The risk assessment process works best when the organization believes in the risk management program's value proposition and fully understands where risk assessment components—such as risk identification and risk prioritization— fit within the overall risk management process. It is incumbent on the owners of the risk assessment process to communicate the next steps, level of effort required, and what the ultimate deliverable will be.

Risk management practitioners often forget that the average person may not understand or appreciate what risk management is or can provide. Risk management terminology can be somewhat arcane, highlighting the negative (i.e., "ineffective", "inability"), and it often is too risk controls focused rather than business strategy focused. In fact, the only time many business managers use risk language is during the annual "check the box" risk assessment.

When we talk about risk management terminology, we mean terms like risk likelihood and impact, management capabilities, inherent risk, risk plans, and risk drivers and consequences. It is important that risk assessment language be operationally relevant and applicable to strategic and business decision-making. This means that defined risks, risk drivers and potential consequences should be highly customized, described in terms specific to the organization and understandable to business management.

Business trends and triggering events driving the need for process improvements

- Board of Director or executive management questions on top risks and the framework to identify, understand and evaluate, mitigate and report risks.
- Challenging business or industry events or trends, and concern over how the risk management program would discover or address risks.
- Changes in senior leadership structure, organization or the business model.
- Confusion over risk assessment roles and responsibilities.
- Concern over ability of existing processes to address recent trends and events such as new market expansion, acquisitions or new product introduction.

Reasons for failure

First, let's define failure. Failure in the case of conducting a risk assessment would be *not meeting the business and corporate expectations* for the risk assessment. Typical expectations for a risk assessment include defining risk terminology and methods, proactively identifying and prioritizing the top risks, assigning risk ownership, conducting targeted analysis on top risks, developing risk plans, and integrating risk management information into business decision-making. These risk process components should result in helping the organization solve business problems and achieve its goals and objectives. When evaluated against those expectations, many risk assessments and risk management processes do not make the cut. Unfortunately, many organizations define success as simply finishing the annual risk assessment, reporting a risk list and heat map, assigning risk to owners and "checking-the-box" until next year.

Key challenges to achieving a successful risk assessment are as follows:

***Planning and communication*–** Poor planning and communication is a large cause for failure because unless a risk assessment has a solid foundation of understanding, the information collected through the effort is likely to not meet expectations. A simple test of the appropriate effort on planning and communication is to spend as much time upfront developing the plan and periodic communication as on the risk prioritization activities and debriefs. A first step is to define the overall risk management program objectives for the organization and key stakeholders. Once that overall step is completed, organizations should tailor the risk program and risk assessment objectives, clearly communicate why the risk assessment is needed, and set expectations for the organization. Risk assessment participants should understand their role in the process and time commitments. Additionally, communication should describe the risk assessment benefits to the participants and the organization (the risk management program stakeholders). Finally, the results of the risk assessment should be communicated on a timely basis to all risk assessment participants, as well as executive management.

Risk inventory structure–Risk inventories often miss important risk categories and risks, and do not reflect current or potential business trends, challenges and strategies. We often see generic risks not tailored to an organization's "language" or business and strategic priorities. A key to success is to describe risks in consistent and understandable terms relevant to the company culture and the risk assessment participants.

Relevance to strategy–The common definition of risk includes both objectives and uncertainties related to achieving business objectives. It is important to consider strategy integration during all risk assessment phases including risk inventory and prioritization criteria development, risk analysis, and risk plan development.

Mismatch in complexity and categorization–Complex risks deserve risk assessment processes that lead to a deep understanding of underlying issues and potential consequences. We often see very complex strategic risks addressed at a level of detail that generates insufficient ownership and plan development. For instance, a common mistake is to describe a risk category as a risk. An example is "human resources risk". Is this one risk or is it a category of risks– a multitude of individual risks such as succession planning, turnover, recruiting, retention, and training? Are there multiple risk owners and risk plans? Are some of the risks more important than others? Often a deep dive analysis on an individual risk can expose important complexities and related interdependencies that can lead to greater success for risk mitigation activities.

Another mismatch can occur in complex organizations. A risk which may be significant in one functional group may not exist in another. Or a risk which is of moderate impact in individual geographies or business units may be very large when aggregated globally. Failure to aggregate and recognize these complexities can undermine the understanding of overall risk exposure and the effectiveness of the risk assessment results.

Prioritization criteria and methods–A common failure is mis-prioritization due to poorly constructed prioritization criteria. One common mistake is to focus on a single criterion such as financial impact effects rather than a combination of quantitative and qualitative criteria covering financial, operational, brand, reputational, and other potential impact factors specific to companies and their industries. Another common methodology fault is providing too narrow an assessment prioritization numerical range–or instance, 1 to 4 which can lead to a central tendency or clustering of results around the middle of the range.

Management capabilities–Many risk assessment processes end after estimating risk severity and likelihood. Risks are prioritized based on the relative size of the risk. This is a valuable exercise for identifying the "big things", but the assessment results paint only part of the picture. The hidden picture is how the risks should be prioritized based on gaps in management's current capabilities to effectively manage the risks. Sometimes the big risks are well managed or even over-managed since people tend to focus on the past as a predictor of the future. We suggest that, in addition to prioritization based on the relative size of the risk, that risks be prioritized based on the "gap" in management capabilities.

Such prioritizing can drive more efficient and objective resource allocation to support appropriate risk-taking and achievement of strategic objectives.

Reporting content and design– The risk assessment information should be complete, easy to understand, and highlight the issues requiring action. From a Board of Directors and senior management perspective, a starting point could be as simple as answering the following questions: "What are the big risks", "Who is responsible" and "What is being done?" A risk prioritization table and heat map can be good first steps, but the keys are to provide insight, depth of understanding, and specifics on what is currently being done and will be done going forward to treat the risk.

Analysis depth–This is often a hidden point of failure, particularly for organizations desiring to only "check the box" to indicate that the assessment has been completed. For a risk related to a key strategic initiative, is just looking at the potential risk impact and likelihood really sufficient? It is possible that the additional information to be gained through qualitative risk analysis methods (e.g., causes and consequences, interdependencies, management capabilities, scenario analysis), could increase levels of understanding of the risk complexities, impacts across the organization, and linkage to strategies and other risk management initiatives.

Risk plans–It is an unfortunate truth that for many organizations, the risk assessment process ends once risks have been identified, prioritized and assigned owners. We believe that the development of comprehensive and specific risk plans is a critical component to a successful risk management program. It is important to understand though that a “plan to develop a risk plan” is not a plan, but a promise, and it should not be confused with effectively managing, monitoring and reporting the risk.

Integration–So what should an organization do with risk management information developed during the risk assessment process? Many organizations collect and organize the information and do exactly *nothing* with the information to make business decisions. We often see little guidance provided on available risk information, appropriate next steps and how the information should be structured and communicated so as to be useful and consumable by management. We believe that risk assessment information can be integrated into many business processes including business and strategic planning, and plans for business expansion, capital investments, mergers or acquisitions, staffing, disaster recovery and crisis management.

Timeliness–Time is the enemy of risk assessments. It is important to time the risk assessment to avoid management distractions or a long period between the risk assessment identification, prioritization, execution and the reporting of the results. A risk assessment is a snapshot of an organization at a point in time, and the information in it can quickly become outdated if the information is not reviewed and approved during a relatively narrow window.

Alternative delivery methods for risk assessments

The three primary delivery methods are risk surveys, facilitated meetings and combination approaches.

Surveys–Risk management surveys are a common and useful method because the application of on-line tools has made the dissemination and data analysis for large surveys very easy to accomplish. There are several points of caution when using surveys.

- The first is to understand that surveys provide a single viewpoint uninfluenced by other opinions. In this narrow communication channel, the challenge is to ask the right risk questions, have the questions understood by the survey respondents, and have the answers correctly interpreted by the survey team. Those are three potential points of failure in a seemingly simple process.

- The second is that the relative ease of use for creating risk surveys has resulted in the tendency of some organizations to think that a larger sample size is a better sample size. It isn’t. For a strategically focused risk assessment, once the survey respondents get beyond the executive and department head levels, the quality of results often drops because survey respondents are providing opinions on topics outside of their organizational knowledge.

- Last, as sample size increases, the results tend to cluster around the middle of the risk prioritization criteria range defeating the goal of identifying a few most important risks on which to focus management attention.

Facilitated sessions–Meetings in which multiple cross functional viewpoints are expressed can create a superior understanding of risks and organizational capabilities to manage risks. One key to successful facilitated sessions is to have experienced facilitators who can encourage positive debate and peer-to-peer cooperation. It is important to understand that the meeting participants may not deal with risk issues on a daily basis, so pre-meeting communication packages and a deliberate meeting pace are important for creating a common initial understanding of key risks.

Combination–Many organizations find risk surveys and facilitated meetings of value and use either or both depending on individual needs. We often see facilitated sessions as part of annual risk assessment update with periodic risk surveys in between to track changing views of risks, identify emerging issues and track risk program performance. Surveys can also be used in conjunction with facilitated sessions to target groups that might not be able to participate in a facilitated session. Some organizations distribute read-ahead materials to stoke the thinking of risk assessment participants to consider how global trends and industry issues impact the organization’s risk profile.

- Typical time commitments include the initial management interviews to identify key business issues, trends and risks as well as time spent responding to surveys, participating in facilitated risk prioritization meetings, and reviewing results.

The total time commitment for most senior management members involved in an annual risk assessment update should not exceed six to eight hours.

Benefits from a successful risk assessment process

- A common risk language including the initial enterprise risk inventory, risk definitions and key risk management concepts (e.g. risk exposure, management effectiveness) to facilitate the discussion of risk across the organization.
- Standardized risk assessment methodology and criteria to be applied consistently across the organization for key risks the organization faces.
- A forward-looking risk profile aligned with strategic goals and objectives as a basis for risk management activities.
- Comprehensive and timely risk action plans with well-defined responsibilities.
- Risk information to support resource allocation.
- A deeper understanding of top risks gained through in-depth risk analysis.
- Risk assessment measures to integrate with existing performance management metrics.
- Better understanding and articulation of business uncertainties and strategies to reduce "organization surprises" and align with strategic goals and objectives.

Alternatives to traditional risk assessments

Risk assessments are a foundational element for risk management programs, and they are a necessary step in the risk management process. However, they can be augmented by a number of methodologies to create a deeper understanding of risks, including risk driver analysis, capability analysis, and risk interrelationship analysis. A methodology that is growing in popularity is risk scenario analysis. Risk simulations using combinations of risk events and trends can generate valuable discussions of the risks and potential management interactions. Risk scenario analysis is most valuable in getting participants to move beyond their initial resistance that low probability events do not deserve management attention. The simulation exercises remove the likelihood debate by stating that the risk event has happened or is happening.

Immediate actions to improve risk assessments

Even the most mature risk management programs often need refinement to promote internal support and excitement, to refresh information to be current and valuable, and to ensure that risk assessment activities are consistent with common standards.

- **First**–*Stop going through the motions.* Risk assessment participants are customers and the risk management program should focus on providing customers with what they want–a risk assessment that provides information valuable for supporting their business decisions.
- **Second**–*Focus on the big things.* Narrow the risk assessment scope through effective risk prioritization methodologies.
- **Third**–*Communicate early and often.* Clearly explain–Why are we conducting this assessment? What is required? What was discovered? How can the risk assessment results support business decisions?

For further information on this topic or the article series, please contact:

Stephen V. Zawoyski
Enterprise Risk Management Leader
stephen.v.zawoyski@us.pwc.com

Michael J. Chagares
Enterprise Risk Management Director
michael.j.chagares@us.pwc.com

Ken Hooper
Enterprise Risk Management Director
ken.hooper@us.pwc.com