Board Perspectives: Risk Oversight

How Mature Are Our Risk Management Capabilities?

Issue 71

Have you ever been asked the question, "How mature is our risk management?" Chances are you have at least heard the question, as we hear it often as well. The presumption is that the more mature a process, the more effective it is. But what does that really mean, and how does the concept of maturity apply to risk management?

Effective enterprise risk management (ERM) enables timely responses to the risks that matter most. There are six elements of risk management infrastructure: (1) policies, (2) processes, (3) people and organization, (4) reports, (5) methodologies and assumptions, and (6) systems and data. An effective risk response considers all of these elements.

Once in place for a given risk (or for a group of related risks), the six elements pave the way for advancing the maturity of risk management. The more mature an organization's risk management, the stronger its culture in balancing the inevitable tension between, on the one hand, creating enterprise value through strategy and driving performance and, on the other hand, protecting enterprise value through a risk appetite framework and effective risk management capabilities.

Key Considerations

A capability maturity framework assists management in thinking more clearly about questions such as:

- Do we rely on a few well-qualified individuals to manage a particular risk in an ad hoc manner, or do we have robust capabilities that we improve continuously?
- How effective do we want our risk management capabilities to be as we improve our infrastructure over time for each of our priority risks?
- Should we vary the rigor and robustness of our risk responses and related control activities by risk type or, alternatively, treat all risks the same in terms of applying mature risk management capabilities?

There are conscious choices to be made when aligning the organization's capabilities with its desired risk responses and vice versa. Given finite resources, risk management capabilities must be selectively improved by considering expected costs and benefits. The goal of ERM is to identify the organization's most significant exposures and uncertainties and focus on improving the capabilities for managing them. That's why an emphasis on risk management infrastructure is important.

The following discussion illustrates five levels of maturity:

- At the *initial state* of maturity, risk management is fragmented and ad hoc. Individual risks are managed

in silos, and the organization is often reactive to events. There is a general lack of policies and formal processes; therefore, the entity is dependent on seasoned managers acting on their own initiative to manage risk.

There is also very little accountability due to the absence of clearly designated risk owners. When personnel leave the organization, the enterprise has difficulty replicating what they do. While the initial state can be rationalized for insignificant risks, the lack of direction is a breeding ground for a crisis in areas requiring more rigor and discipline.

- At the *repeatable state* of maturity, basic risk management policy structures and processes, including risk assessment, are in place to achieve stated objectives and requirements. Human resources are allocated to risk management, with responsibilities and authorities defined for specific individuals. Accountability may still be an issue at this stage because reporting is not rigorous enough to hold specific individuals accountable for results. Thus, there is still heavy reliance on people to "take care of things." However, when someone leaves, the void is not as great now that "repetition" is taking place as a result of increased process discipline and established guidelines for managing risks.
- At the *defined state*, policies and processes are further refined and documented, resulting in more uniform risk mitigation activities and risk oversight across units and functions. For example:
  - A risk committee structure may be in place, along with a designated executive responsible for aggregating enterprise risks and ensuring cross-unit and cross-functional coordination.
  - Robust controls documentation and verification mechanisms are in place to ensure policies are followed and processes are performing as intended.
  - Roles and responsibilities are clearly defined. Robust management reports, supported by rigorous methodologies, add more value by integrating appropriate key performance and risk indicators into decision-making processes.
  - Systems are more stable and scalable with improved functionality because technology lays a foundation for all of the other infrastructure elements.
  - There is evidence of "risk-sensitive and risk-aware decision-making," as exceptions and "near misses" are reported in a timely manner, and lessons learned and control deficiencies drive improvement initiatives.
- Organizations functioning at the defined state are building the foundation for a strong risk governance and culture. At the *managed state*, we see improved quantification, time-tested models and data analytics assisting decision-makers with forecasting, scenario-planning and trend analysis to identify emerging risks and anticipate the potential for disruptive change. A formal lines-of-defense framework is implemented, risk measures are linked to performance goals, early warning systems are in place, and capital allocation techniques are effectively deployed.

  A risk appetite framework also is established and decomposed into risk limits allocated to operating units. When predefined limits are approached or exceeded, the situation is evaluated and corrective action, if needed, is taken. Objectives, targets and performance metrics are integrated into enterprise-wide systems providing dashboard reporting and drill-down capabilities. These enhanced capabilities facilitate the integration of risk considerations into strategy-setting, business planning and performance management; they also position the organization as an early mover to recognize and act on emerging risks (as well as opportunities).
- The *optimizing state* is the highest level of capability, in which the organization has a commitment to improve the capabilities at the managed state continuously, keeping all elements of risk management infrastructure fully aligned as the business environment changes. Risk policies are evaluated on an enterprisewide basis to achieve the desired risk/reward balance, as well as to understand and exploit the effects of diversification across multiple risks.

  In the optimizing state, best practices are routinely identified and shared across the organization,

suggesting that the journey of enhancing risk management capabilities continues over time as external and internal conditions change. Corporate improvement initiatives established and applied enterprisewide (e.g., Six Sigma) are integrated with risk management.

These are the five stages of a capability maturity framework. The illustrative criteria above shows how each successive stage of maturity reflects further enhancements in managing risk. The more mature a company's capabilities, the greater its prospects for success in managing risk and the lower its potential for failure. A consistent and fact-based use of a capability maturity framework by risk owners allows for a focused understanding and articulation of the current and desired states of risk management capabilities across the organization.

To illustrate, a maturity framework works as follows:

- For each risk (e.g., regulatory, health and safety, or supply chain risk), evaluate the current state of the entity's risk management capabilities. The *current state* generally refers to capabilities that are present and functioning, but it may take into account *planned initiatives* currently funded and under way to improve capabilities (also known as the *improved state*).
- Decide how much added capability is needed to achieve the appropriate risk response: *the desired state.* When assessing the desired state, be as realistic as possible. The objective is to select capabilities that provide the best fit with the core competencies that would be reasonably expected of an organization executing the enterprise's business model.
- Recognize that the desired state capability may vary by risk. For example, significant exposure to changes in foreign exchange rates may require capabilities at least at the *managed state.* Some operational risks, such as operating a nuclear power plant, may drive management to choose the *optimizing state* because there is little margin for error in operation. Windstorms, flooding and other hazard risks may only warrant periodic analysis and procurement of insurance with little need for intricate risk reporting – *a repeatable state* capability. For cybersecurity risks involving "crown jewel" information assets and systems, a *managed state* may be desired.
- Once the gap between the current state and desired state is identified, evaluate the expected costs and benefits of increasing capabilities to close the gap. The actionable steps resulting from a gap analysis become an integral part of the business plan.

Improvements in capability are often "staged." To illustrate, assume the current state of a company's credit risk management capabilities lies at the repeatable state. Assume further that management decides that these capabilities should operate at the managed state. In closing this gap, it may be preferable to use a staged approach to the design and implementation of improved capabilities by first advancing capabilities to the defined state and then to the managed state, rather than closing the gap all at once.

This approach reduces disruption to the organization, as it may be more in line with the change readiness of the entity's personnel and may even increase the chances of a successful implementation. Thus, the capability maturity framework facilitates careful thought and judgment by knowledgeable personnel in planning and also determining the speed of the organization's transition from the current state to the desired future state.

There is no one-size-fits-all. What constitutes "best practice" in managing a particular risk at one company may be insufficient or overdone in the context of managing the same risk at another company. For example, sophisticated modeling applications may represent best practice for managing market risk in a trading organization. However, in another business where just a handful of transactions are exposed to price risk, such sophistication is unnecessary because of the negligible exposure. It is unnecessary to deploy the most advanced techniques for all risks. No organization has the resources to do that, nor is there a viable business reason to do so. Thus, thinking in terms of capability maturity can facilitate the resource allocation process.

Questions for Boards

The following are some suggested questions that boards of directors may consider, based on the risks inherent in the entity's operations:

- At what stage of maturity are our organization's risk management capabilities, both for the enterprise as a whole and for each of our most critical risks?
- Do our organization's risk responses to address individual risks reflect a careful assessment of the appropriate capabilities needed to reduce risk to an acceptable level?
- If our risk management capabilities require improvement, do we have a plan to take them to the next level of maturity?
- Are we over-reliant on our people to manage some of our critical risks and, therefore, exposed in the event of an unexpected departure or termination?

How Protiviti Can Help

Protiviti assists directors in public and private companies to identify and manage the organization's key risks. We provide an experienced, unbiased perspective separate from those of company insiders in evaluating the maturity of risk management capabilities.

About Protiviti

Protiviti (**www.protiviti.com**) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. Protiviti and our independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Named one of the 2015 *Fortune* 100 Best Companies to Work For®, Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Protiviti is partnering with the National Association of Corporate Directors (NACD) to publish articles of interest to boardroom executives related to effective or emerging practices on the many aspects of risk oversight. As of January 2013, NACD has been publishing online contributed articles from Protiviti, with the content featured on www.nacdonline.org/Magazine/author.cfm?ItemNumber=9721. Twice per year, the six most recent issues of *Board Perspectives: Risk Oversight* will be consolidated into a printed booklet that will be co-branded with NACD. Protiviti will also post these articles at **Protiviti.com.**

protiviti®
Risk & Business Consulting.
Internal Audit.