Office of Risk Management and Analysis

Risk Management Practices in the Public and Private Sector: Executive Summary

September 2010

Homeland Security
This publication is presented on behalf of the Office of Risk Management and Analysis, National Protection and Programs Directorate, United States Department of Homeland Security. The Office of Risk Management and Analysis (RMA), works to ensure that risk information and analysis are provided to inform a full range of homeland security decisions, including strategy formulation, preparedness priorities, and resource allocation. Specifically, RMA provides risk analysis, enhances the risk management capabilities of its partners, and integrates homeland security risk management approaches.

For more information about RMA, please contact 202-343-4000 or risk_management@hq.dhs.gov
Summary

The Department of Homeland Security (DHS) Office of Risk Management and Analysis (RMA) conducted a study of risk management practices in public and private organizations between May and July 2010. The purpose of the study was to help guide RMA and Risk Steering Committee (RSC) efforts to build a risk management program for DHS. The study consisted of over 20 one-hour interviews with executive-level risk practitioners at Fortune 500 companies, staff-level risk practitioners at government agencies, and individuals from other organizations who are familiar with risk management.

The study’s key findings can be characterized in three areas:

1) How risk management and analysis is being integrated across organizations;

2) How risk management activities are aligned to organizations’ structures and processes; and

3) Methods that organizations use to improve the conduct and communication of risk analysis.

As the RSC continues to lead in the efforts to build an integrated risk management program at DHS, it should consider the common practices and lessons learned identified by RMA via this study.

Integration of Risk Management and Analysis

Many of the interviewees said they were seeking to integrate the management and analysis of risk across their organization. This was particularly true in the private sector, although several public sector organizations were seeking to do so as well. The study found organizations employed several tactics.

- Organizations are increasingly seeking to understand and manage risk on a holistic, enterprise-wide level. Numerous interviewees, particularly in the private sector, expressed a desire to understand risk in an integrated manner as the driver for the development of their risk management programs. They said that it was a priority of their leadership to understand how risks affected their entire organization. The interviewees noted that risk management strategies could affect their business units unequally, and that a good decision for one business unit could be a bad decision for another. They also said that without an enterprise-wide understanding of risk, business units may accept more risk than the organization’s leadership is willing to accept, either on an individual or collective basis.

- Risk is commonly understood and assessed as it relates to an organization’s objectives. The vast majority of interviewees said their organizations consider risks in relation to how it affects the organization’s ability to achieve its objectives. Thus, they saw the value of risk management as helping to maximize an organization’s ability to achieve its objectives. One interviewee said he thinks “enterprise risk management is enterprise goal management.”

- Risk management is incorporated into strategic planning. Almost every participant in the study recognized the importance of linking strategic planning and risk management, although not every
participant said they had done so successfully at their organization. Of those interviewees who did not feel they had done so successfully, most said it was a priority to do so next year. One participant in the study reinforced this focus, saying “strategy and risk need to be playing the same game.”

- **Organizations regularly track and monitor the risks they face.** The majority of interviewees RMA spoke to were looking for ways to monitor and track their organizations’ risks. They desired to do more than conduct a periodic risk assessment. Participants wanted to find factors that were correlated to their organizations’ risks, which could be tracked on a more regular basis and give warning that exposure to risks were changing.

- **An organization’s leadership must be aware of its risks.** Study participants emphasized that it is important that an organization’s leadership be aware of its risks. They expressed concerns that if there were layers between risk information and leadership, then the risk information could be censored before leadership had a chance to review it. Most interviewees said risk executives should have either direct access or regular meetings with key leaders, such as a Chief Executive Officer or Board of Directors.

- **Organizations attempt to facilitate cascading communication of risk.** Many interviewees emphasized that risk information should flow up, down, and across their organization. In general, the leadership of the organization is responsible for communicating strategic direction regarding risk, such as those risks that leaders wanted to prioritize managing. Interviewees said business units and project managers were responsible for using this information to develop implementation strategies. Interviewees emphasized that leadership could not set its priorities, however, without understanding the risks that their business units and project managers face. As a result, interviewees said that it was important that the business units and project managers communicate risks to leadership, particularly when changing situations could merit altering risk management strategies.

**Organizational Alignment**

There were several commonalities in the manner organizations structured themselves to manage and analyze risks most effectively. Some of these structural decisions lend themselves to better understanding and communicating risks, while others were to reinforce the aforementioned desire to analyze and manage risk in an integrated fashion.

- **Organizations customize risk management programs to fit their needs and culture.** One of the key points many interviewees emphasized was that there was not a standard model for a risk management program at an organization. Each organization had different contexts through which their risk management programs were designed and implemented. While they acknowledged general standards that were used in the development of their risk management programs, interviewees noted that it is important that a risk management program match the culture and operations of the organization it is designed to serve.

- **Leaders at the executive level must endorse and sponsor a risk management program.** Interviewees repeatedly emphasized the importance of executive sponsorship of a risk
management program. They noted that risk management programs require participation at all levels of an organization, and said executive sponsorship encourages that participation. Furthermore, many participants noted that a risk management program is only effective if it is used to inform decision making. This means that leaders must support the program and incorporate the information coming from it when they are making decisions.

• **Accountability for risk management should be clearly defined and risks should be managed by the unit closest to the risks.** It was clear during the interviews that many organizations with well developed risk management programs had clearly defined who in the organization was accountable for actually managing risks. In fact, many interviewees indicated that during the initial implementation of their risk management program, one of their first steps was to define accountability in their organization for what business units or executives were responsible for managing identified risks. Furthermore, interviewees often said that the term risk “management” was misleading when discussing the role of their central risk offices. They said business units at their organizations were largely responsible for making risk management decisions. This is because the business units often have the most knowledge about the risks they face and how to control these risks.

• **Central risk management offices and committees have been established at many organizations.** Organizations that want to understand their risks in a holistic, enterprise-wide manner have established central risk management offices and committees to facilitate doing so. In general, interviewees said the offices and committees share the responsibilities of overseeing their organizations’ process for identifying, assessing, and managing risk, creating tools and trainings to help business units with those processes, facilitating enterprise-wide discussions and decisions about cross cutting risks, monitoring indicators related to risk, briefing organizational leadership about risk, and identifying emerging risks. The committees generally include decision makers, meet on a regular basis, and are often chaired by a high ranking executive such as the CEO. They are predominantly tasked with considering how risks affect the enterprise as a whole and overseeing risk issues at the organization.

• **Risk management programs are facilitated by an executive at the organization.** Interviewees at organizations that have central risk management programs usually said their organization tasked an executive with facilitating the implementation of the risk management program. The placement of these executives varied widely from organization to organization, but most had similar responsibilities. These responsibilities tended to be very similar to those of central risk management offices: to oversee the organization’s risk management processes, to act as a sponsor for risk management, and to work with parts of the organization to improve risk management capabilities. However, interviewees cautioned that it was not enough to simply have an executive tasked with overseeing the organization’s risk management framework—the organization must act on the framework as well.

• **Many programs start with a limited scope.** When initially developing a risk management program, many interviewees said they started with a limited program. They pointed to a number of factors driving this, including limited resources, a desire to prove value before expanding, and the number of risks that would need to be considered if a program

> “Chief risk officers are a symbol of risk management, not a panacea.”
> -Interviewee, 2010
is not bounded. However, these interviewees usually said they worked to broaden the scope of their risk management programs after the initial implementation.

- **Organizations rely on comparative studies and maturity models to assess their risk management capabilities.** Organizations that are looking to consider the maturity of their risk management programs tend to measure themselves using standards developed by organizations like the Committee of Sponsoring Organizations (COSO) or the International Organization for Standards (ISO), or through comparative studies to other organizations. Many organizations also use “maturity models” to measure their risk management capabilities. However, interviewees were not able to point to a common benchmark standard that organizations could use to assess their relative maturity.

- **Organizations should work to instill a culture of risk management throughout its staff.** Many interviewees made the point that a risk management program can only be successful if the principles of risk management are adopted by the organization. These participants emphasized that their goal was not to generate a risk management program that sat outside the organization’s standard management processes, but was instead incorporated into those processes. Therefore, the emphasis of risk management efforts should not just be on developing a well functioning and efficient risk management program, but also to change the approach members of the organization take when making decisions.

### Risk Analysis Methods
There were also several common methods and principles interviewees mentioned when they analyze and communicate risk at their organizations. They said these methods were important to ensure decision makers understood risk analyses and were enabled to make risk-informed decisions.

- **Risk practitioners attempt to present risk in a simple and relevant manner.** Numerous participants in the study emphasized that risk information must be presented in a simple and relevant way. They warned that risk practitioners must not present information in a technocratic manner, lest their recommendations be misunderstood or ignored. Interviewees said that risk analyses should only be as complicated as the decisions they seek to inform and the data that is available to analyze. In addition, study participants said it was important that decision makers understand the relevance of the risk information.

- **There are few strong metrics to measure the success of risk management programs.** Every participant in the study, who was asked, said they had difficulty in developing metrics that can be used to assess a risk management program. They said the benefits of risk management could largely only be assessed on a qualitative basis, as attempting to illustrate that an organization avoided risks is proving a negative. Some participants did point to some factors that can be used to measure a risk management program, however. Some interviewees proposed output-type measures such as whether a risk management decision process is being used, while others proposed proxy measures such as the number of surprise risk events that affect an organization.

“[Risk analysts sometimes] get too focused on the deliverable.”

-Interviewee, 2010

-5-
• **Formal risk positions are difficult to establish, but it is important for an organization to attempt to do so.** Organizations often have trouble explicitly determining a position for the amount of risk they are willing to accept that could affect their ability to achieve their goals. This is similar to the concepts of setting a risk appetite, risk tolerance, or risk threshold. Many interviewees said they could not set an explicit risk position due to concerns from their legal departments or a simple unwillingness of leadership to say they were willing to accept risks. However, most study participants believed organizations should establish a risk position.

• **The identification of emerging risks is a priority for many organizations.** Many study participants from the private sector said the identification of emerging risks is a key risk management process. These participants noted that a key value of risk management is to help an organization anticipate risks before they happen. Although risk managers cannot see into the future and will likely not be able to anticipate every risk that could affect a company, they said risk managers should try to provide their leadership with as much warning as possible about new risks that could affect the organization.

• **When identifying and assessing risk, it is important to provide anonymity.** Many interviewees expressed a belief that anonymity is important when attempting to identify and assess risk. They identified several reasons for this, such as the danger of developing a groupthink and individuals’ fear to mention risks or mistakes to regulators or leaders. These participants took great pains to provide anonymity to people in their organizations who participate in risk identification and assessment.

• **Practitioners should encourage diversity of thought when considering risk.** Several participants indicated that diversity of thought was not only important for risk assessment, but also a key benefit of risk management. They said risk analyses are only as good as the cross section of individuals involved in the process, to ensure a wide range of backgrounds and viewpoints were incorporated into the analyses.
Contrasts between Public and Private Sectors

Since this study included interviews with personnel from both the public and private sector, it was possible to identify contrasts in risk management approaches between the two types of organizations. Some of these contrasts were manifestations of complications due to the differing nature of organizational purpose in the two sectors, while others were areas where the public sector seemed to simply lag behind the private sector. These contrasts included:

- **Securing consistent, ongoing support from leadership.** A key success factor identified by study participants in the public and private sector was sponsorship and support for executive leadership at an organization. However, numerous participants from the public sector expressed difficulty in achieving consistent support. Many of these participants linked this to the high rate of turnover among the political appointees tasked with leading Federal agencies (appointees have a median tenure of 2.5 years). Several participants reported having efforts to implement a risk management program derailed because of leadership changes at their organization.

- **Responsibility for managing politically controversial risks.** Other public sector participants reported problems implementing risk management programs when dealing with risks that had politically controversial implications. These are generally risks that private sector organizations do not face because they have different mandates than government agencies, or risks that they rely on the government to manage. There were a number of reasons for these problems. First, many said leaders were unwilling to consider risk management principles when considering these issues, such as risk positions or tradeoffs. For example, one participant said leaders at the agency were unwilling to say they would accept risks to the safety of their personnel. Interviewees also said that legislative mandates interfered with their ability to manage risk.

- **Managing risk at an enterprise-wide level.** The most significant difference between public and private sector approaches to risk management was how broadly risk management programs operated across an organization. Many private companies RMA met with were trying to understand and manage their risks on a holistic, enterprise-wide basis while many public agencies were managing risks on an uncoordinated, ad hoc basis. For example, attempts to coordinate interviews with participants from one government agency were complicated by the fact that disparate groups were responsible for overseeing the management of related risks.

- **Linking risk management to achieving objectives.** The lack of a link between risk management and an agency’s ability to achieve its objectives could be related to why the public sector has lagged behind the private sector in adopting enterprise risk management. Notably, the two government entities we spoke to that were seeking to manage risk on an enterprise-wide basis were exceptions to this, suggesting a correlation. Many of the Federal agencies focused on risk simply as uncertainty or bad things that could happen to the agency or the public.
Next Steps

In May 2010, Secretary of Homeland Security Janet Napolitano signed the DHS Policy on Integrated Risk Management, directing the RSC and RMA to lead efforts to develop the Department’s risk management capabilities. This was also identified as a key initiative in the Bottom-Up Review, an assessment of the Department’s activities against the goals in the Quadrennial Homeland Security Review. As the RSC and RMA work to develop the Department’s risk management capabilities, they will evaluate the findings of this study and attempt to incorporate those practices that would improve the Department’s risk management program.

As most interviewees emphasized, there is no “one-size-fits-all” approach for implementing risk management at an organization, so DHS will seek to implement only those findings that match the Department’s needs and culture. Additionally, since the field of risk management is constantly evolving, DHS will revisit these findings periodically and continue to monitor evolving practices. Finally, DHS will enhance and expand its partnerships with public and private risk management practitioners so that it may continue to benefit from their experience and insight.