Deloitte.

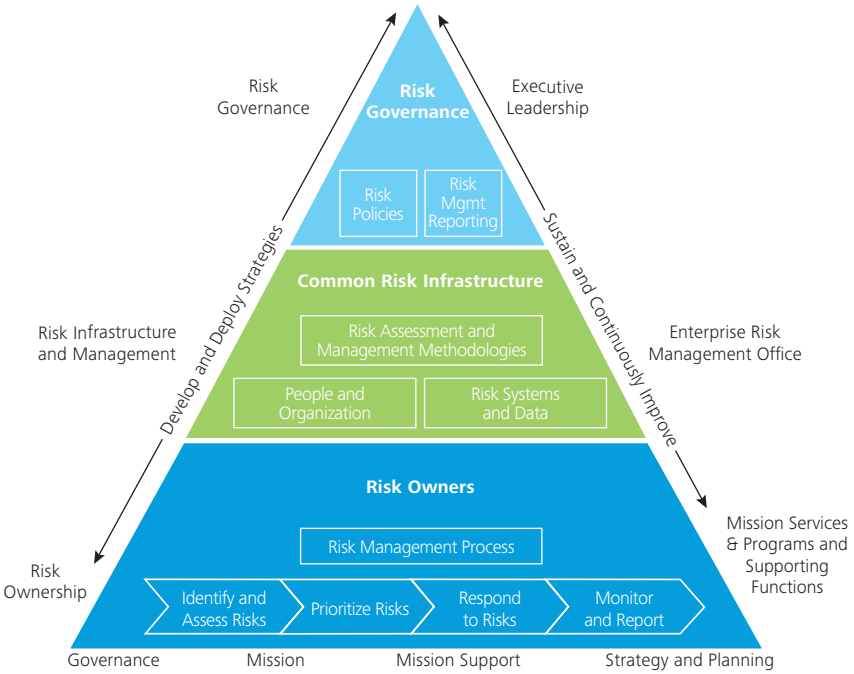
Federal CFO Insights
Risk intelligent risk committees for Federal executives

Introduction: Risk committees become reality

Like other enterprises, federal agencies are under intense pressure to manage strategic, regulatory, security and reputational risks. But in some ways, federal risk oversight can be even more complex than the challenge faced by private corporate boards. How do cabinet secretaries and other senior leaders gain the clear view they need to uphold public trust and congressional expectations when departmental risk management is widely dispersed among large, often independent, administrations?

While risk management is not new to federal agencies, senior executives at many agencies are refreshing their thinking with regard to risk governance and oversight. Agencies weigh the advantages of a centralized body dedicated to risk management with the cost of operating a whole team. To support their risk management activities, some federal agencies have established risk committees. These agencies regularly revisit their risk committee charters and activities to ascertain that the risk committee has the composition, reporting relationships, and responsibilities that best suit the enterprise.

Risk Intelligent Enterprise™ framework



Deloitte's concept of the Risk Intelligent Enterprise™ exemplifies Deloitte's approach to risk (see below). The "pyramid" below depicts the framework of the Risk Intelligent Enterprise that portrays the relationship between Executive Leadership, the Enterprise Risk Management Office, and the Mission Services & Programs and supporting functions, and their risk-related responsibilities.

The primary role of the risk committee is to provide a common point of risk oversight or risk governance for the organization. The risk committee's role should not be positioned as a surrogate for risk management accountability, which would still reside at with the respective managers responsible for assigned functions, programs and projects.

This article first presents considerations for senior executives contemplating the formation of a risk committee (Section 1). It then covers topics that a risk committee charter might include, given that the charter describes the responsibilities of the committee, as well as tips on developing and using the charter (Section 2). Next, we provide suggestions related to how a risk committee may go about fulfilling its chief responsibilities (Section 3) and educating and evaluating itself (Section 4).

Section 1: Considerations in forming a risk committee

Senior executives at federal agencies might consider the following key factors in deciding whether to form a risk committee:

- **The needs of stakeholders:** The risk-related needs of the agency and its stakeholders should be considered. In the process, senior executives might assess the quality and comprehensiveness of the current risk governance and oversight structure, the risk environment, and the future needs of the agency. The composition and activities of the risk committee and its relationship with other committees should reflect senior executives' assessment of those factors.

- **Alignment of risk governance with strategy:** Senior executives should consider whether risk oversight and management are aligned with the agency's mission and strategy.

- **Oversight of the risk management infrastructure:** It is useful to consider whether the risk committee would be responsible for overseeing the risk management infrastructure — the people, processes, and resources of the risk management program — or whether another committee will oversee that infrastructure.

- **Scope of risk committee responsibilities:** Senior executives may need to decide whether the risk committee will be responsible for overseeing all risks, or whether other committees will be responsible for some. It is also important to consider how the interrelatedness of risks will be assessed and addressed.

- **Risk-related communication:** Senior executives should consider how the committees will keep one another — and other leadership — informed about risks and risk-oversight practices. Efficiency and effectiveness call for clear boundaries, communication channels, and handoff points. This need may require senior executives to define these elements clearly, making adjustments as needed.

Section 2: Risk committee charter and composition

The risk committee defines its role in risk governance by means of the risk committee charter. In writing the charter, executive leadership and the risk committee will determine the risk committee's role in risk governance. The risk committee charter defines senior executives' involvement in and approach to risk oversight. In developing risk committee charters, senior executives may wish to consider including language that specifies:

- The separate nature of the risk committee and its purpose of exercising enterprise-wide risk oversight.

- The reporting relationships between the risk committee, and program and project management.

- Who is responsible for establishing the criteria for office, program and project management's reporting about risk to senior executives (although the actual criteria need not be set in the charter, because they can be expected to change as mission priorities and risk factors change).

- The composition of the risk committee and the qualifications of risk committee members.

Regarding specific risk-oversight responsibilities of the committee and how it fulfills them, senior executives may also want to specify the following:

- The risk committee's responsibilities regarding the agency's risk appetite, risk tolerances, and utilization of the risk appetite.

- The risk committee's responsibility to oversee risk exposures and risk strategy for broadly defined risks, including for example operational, compliance, legal, property, security, IT, and reputational risks.

- The risk committee's responsibility to oversee the identification, assessment, and monitoring of risk on an ongoing agency-wide and individual-entity (for example project, program, or department) basis:

- The risk committee's responsibility for assessing the agency's actual risk appetite over time.

- The risk committee's oversight of office, program and project management's implementation of the risk management strategy.

In general, the more precise the charter, the better positioned the risk committee will be to exercise oversight. For example, a detailed charter should enable the committee to develop an annual meeting calendar, based on the responsibilities and required meeting frequency. The calendar might include specific risk issues (such as risk appetite) and activities (such as risk committee education) for discussion, as well as meeting agendas, using the responsibilities in the charter as a guide.

In addition, it may be appropriate to coordinate the risk committee calendar with those of other committees so that the risk committee should, at a minimum, be made aware of the risk-related activities of those committees. Coordinating their calendars enables the committees to coordinate their activities and their use of resources to maximize risk-oversight efficiency.

Section 3: Fulfilling risk-oversight responsibilities

Effective risk oversight depends on the way in which the risk committee fulfills its responsibilities and interacts with the executive leadership and stakeholders. Broadly, the responsibilities of a risk committee may include the following:

- **Oversee the risk management infrastructure:** Agency leadership may oversee the agency's risk management infrastructure, or this oversight responsibility can be delegated to a risk committee.

- **Address risk and strategy simultaneously:** Address risk management and governance when strategies are being created and program and project management decisions are being made. The purpose is typically not to promote risk avoidance, but to promote informed risk taking in support of the agency's mission in the context of sound risk governance.

- **Assist with risk appetite and tolerance:** The risk committee can help establish, communicate, and monitor the risk culture, risk appetite, risk tolerances, and risk management capabilities of the agency at the office, program and project levels.

- **Monitor risks:** The committee should assist in assessing and monitoring the agency's compliance with the risk management policies and defined risk tolerance boundaries. Additionally, the committee should play an active role in understanding and gaining assurance on the effectiveness of risk response or mitigation strategies. For the risk committee, this responsibility extends to all risks, or at least to all risks not monitored by other executive committees. In cases of risks monitored by other executive committees, the risk committee should be made aware of such ongoing risks and related risk response strategies.

- **Oversee risk exposures:** The risk committee requires visibility into critical risks and exposures and into program and project management's strategy for addressing them. The committee should consider the full range of risks and potential interactions among risks, as well as risk concentrations, escalating and de-escalating risks, contingent risks, and inherent and residual risk.

- **Advise senior executives on risk strategy:** The risk committee should serve as a repository of information and expertise on risk and be positioned to advise senior executives on risk strategy, risk exposures, and risk management.

- **Consult external experts:** As needed, the risk committee should access external expert advice regarding risk, risk governance, and risk management in the form of meetings, presentations, verbal or written briefings, or commissioned projects. Areas to cover could include the risk environment, regulatory developments, leading practices, or other items senior executives or committee members specify. It is appropriate for the risk committee to seek external education regarding risk management or compliance matters, evaluation of the risk infrastructure, or assessment of its own practices.

Senior executives and the risk committee can assert responsibilities in any given area by writing them into the risk committee charter. In addition to the above responsibilities, the risk committee might also consider the following:

- **Locate gaps and overlaps:** Given its enterprise-wide view of risk, the risk committee is positioned to locate gaps and points of overlap between department and agency committees. If any are discovered, the committee may be positioned to recommend ways to address them and define or redefine appropriate boundaries and communication channels.

- **Define risk reporting parameters:** The committee should consider how to define significant decisions, transactions, funding, and other items that program and project management should bring to the risk committee's and senior executives' attention. These may be defined by type, amount of exposure, and any other criteria the risk committee specifies.

- **Provide adequate funding:** The risk committee can also influence the adequacy of budgets and resources for risk governance and risk management.

- **Recognize IT's role:** IT is integral to risk management and oversight in every agency. Given this, the risk committee should understand the role of IT in the risk management infrastructure and the risks to IT, including those posed by cybercrime and other cyber threats.

- **Review crisis management plans:** The committee should keep abreast of crisis preparedness and ascertain that program and project management has developed and can implement a plan to respond to major risks, such as natural disasters, terrorism, cyber attacks, epidemics, civil disorder, and other events that could compromise the agency's human resources.

Section 4: Ongoing education and periodic evaluation

As with other executive responsibilities, risk oversight is not a set-it-and-forget-it proposition. Risks in the economic, regulatory, and technological environments are dynamic, and risk governance should evolve in response.

As a relatively new committee dealing with an area in constant flux, the risk committee should consider how it plans to stay informed about developments in risk management practices. The following guidelines can assist risk committees in developing education and training initiatives to:

- Stay abreast of leading practices as risks evolve and as program and project management updates its risk management methods.

- Provide orientation programs for new risk committee members and a module in executive leadership's orientation to inform them about the risk committee.

Education could include sources ranging from conferences and continued readings to courses designed for senior executives to customized briefings from external specialists. Deloitte suggests a mix of general updates and agency-specific information on risk, risk governance, and risk management.

It may be advantageous to periodically evaluate the performance of the risk committee as a whole and, possibly, that of individual members.

Areas of risk committee performance to consider evaluating may include:

- Breadth and depth of the committee's knowledge of risk, risk governance and risk management (and the effectiveness of ongoing education)
- Performance of the chair of the committee and his or her relations with the committee
- Clarity of communications about risk and the degree to which these communications have been understood and acted upon
- Quality of risk committee responses to potential or actual financial, operational, or other risk events
- Relevance and usefulness of the information
- Received and of reporting about risk by program and project management

There are several methods for executive committee evaluations, each with its advantages and disadvantages:

- Self evaluation
- Peer evaluation
- External evaluation

Conclusion: Ever vigilant, continually improving

Much of the value of the risk committee will likely come from the questions it poses, such as the following, which are central to risk oversight:

- What are all the risks of a decision or initiative — for instance, of a new project, program, or strategic initiative — that the agency may be considering?
- What are the new or emerging risks the agency should consider as a result of changes in its programs, services, leadership, systems, processes, and any external factors impacting the organizations mission?
- What steps have been taken to mitigate, manage, and monitor those risks? Who is accountable for managing each the most critical risks for the agency?

Developments in the financial, economic, and regulatory environment can be expected to subject risk committees to an expanding range of responsibilities, up to and including weighing in on strategic issues from a risk-oversight perspective. While the executive leadership takes the lead in strategy discussions, the risk committee will have a valuable perspective to offer.

Regardless of how the committee's responsibilities evolve, a key skill of its members will be to understand and prioritize the risk governance and oversight needs of the agency. This can require at least as much wisdom as skill. By that, we mean committee members should understand the risks posed by the agency's mission and by external forces and how they might affect the mission and the agency itself. The committee should question program and project management about the risks and about how the agency is addressing them. Then they should listen carefully to the answers and, as appropriate, probe for more information.

Further information may come from internal financial and operational reports and from informal conversations. In fact, when failures in risk management occur, in Deloitte's experience, post-incident reviews of "What happened?" often reveal that information that could have helped the enterprise recognize the risk sooner and address it more effectively already existed within the agency.

Questions to ask to encourage continual improvement in risk oversight:

- How do we evaluate candidates for senior positions in terms of their risk awareness and approach to risk management?
- How are we helping to drive a more risk aware culture that is focused on improving outcomes related to the agency's programs, services, and initiatives?
- What are our evolving ethical and legal responsibilities for risk oversight in energy efficiency, water usage, labor practices, and other areas of sustainability, and how are we meeting them?
- Where is the line between risk oversight and risk management? How do we practice the right balance that characterizes sound risk governance?
- How do we keep the risk committee from becoming stale, set in its ways, or merely pro forma in its approach to oversight? How do we stay open to opportunities to improve when we believe our methods are working?

This presents risk committee members with a real opportunity. They can shoulder the responsibility of helping program and project management to identify not only risks and ways of addressing them, but also ways of improving the risk management infrastructure so that information about risks and how to manage them surfaces before, rather than after, risk events.

Primary contacts

Marc Greathouse
Partner
+1 571 814 7370
margreathouse@deloitte.com

Don Dixon
Director
+1 919 546 8112
dodixon@deloitte.com

Ian Waxman
Senior Manager
+1 215 405 5551
iwaxman@deloitte.com

Deloitte *Federal CFO Insights* are developed with the guidance of Roger Hill, Principal, Federal CFO Program Leader, Deloitte & Touche LLP; and Philippe Podhorecki, Manager, Federal CFO Program, Deloitte Consulting LLP

About Deloitte's Federal CFO Program
The Federal CFO Program brings together a multidisciplinary team of Deloitte leaders and subject matter specialists to help Federal finance leaders stay ahead in the face of growing challenges and demands. The Program harnesses our organization's broad capabilities to deliver forward thinking and fresh insights for every stage of a leader's career — helping Federal CFOs manage the complexities of their roles, tackle their company's or agency's most compelling challenges, and adapt to strategic shifts in the market.

For more information about Deloitte's Federal CFO Program, visit our website at www.deloitte.com/us/FederalCFO.