Deloitte.

Times are changing: Risk identification and effective management

The increasing risk of enterprise-level threats to federal agencies should be a catalyst for change. But it also has the potential to be deeply disruptive, leading to uncertainty and inefficiency. The effects of troubling new threats to operational security can be disabling, at a time when some vulnerabilities are going unchecked or unidentified at the federal level.

This is all the more problematic since many federal agencies believe that they have a good handle on their risk exposure, and the plans they have in place to manage it. It can create a false sense of security that may put the agency's mission at risk while clouding leadership decisions and priorities.

How do federal organizations bridge the gap between timely identification of emerging risks and effectively responding to them so as to avoid operational disruption?

Those hoping to capitalize on the advantages of change while preventing or mitigating threats should become active managers of many types of risk, particularly those that can truly impact an organization's ability to fulfill its mission. To do this, federal agencies need to anticipate future threats to the core mission and related support activities. They should also have defined and repeatable processes in place to actively assist leadership with anticipating, identifying, and managing risks, as opposed to waiting to respond to risks once they occur. Risk management should not be an ad-hoc process or based on the assumption that managers doing their jobs will always know and manage risk. Figure 1, below, provides a more intentional and robust approach to consistently managing risks across the enterprise.

New threats are dramatically changing for federal agencies

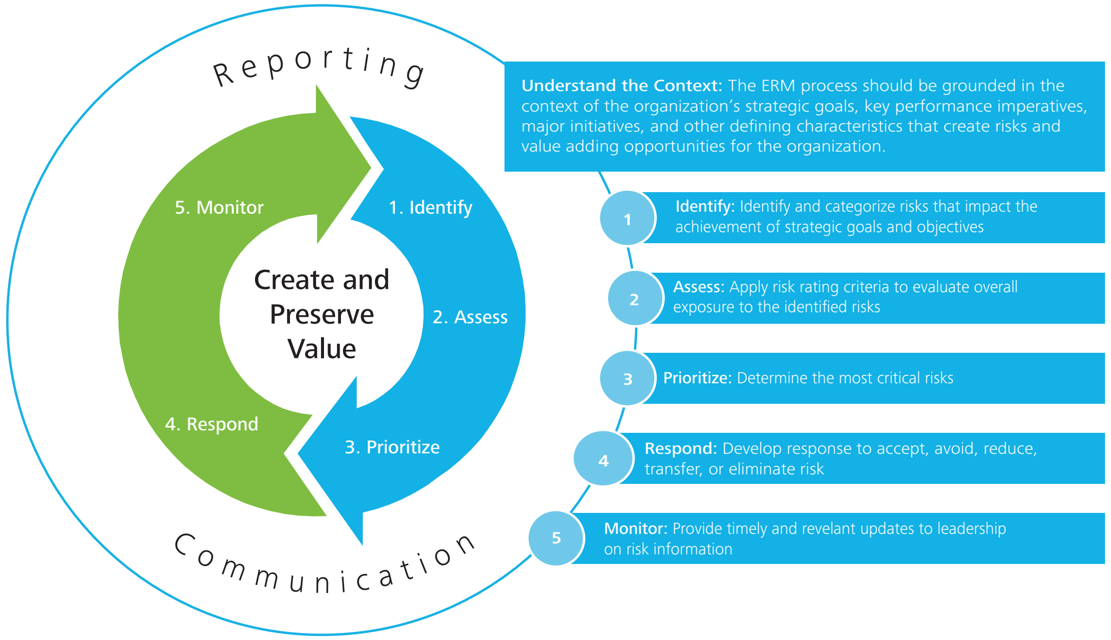
"Security and warfare look very different in 2020. Electronic intelligence and surveillance functions driven by big data have become key defense requirements"…" An upsurge in cyber-warfare makes it increasingly difficult to distinguish between the actions of terrorists, organized criminals, fringe movements, nation states, and teenage hackers."

"Economic losses from cyber-attacks rise to $3 trillion by 2020."

"Governments apply the consulting staffing model to their workforces. Permanent employees undertake a wide variety of creative, problem-focused work in a virtual staffing cloud. Government workers vary in background and expertise but exhibit traits of "free agents"—self-sufficiency, self-motivation and a strong loyalty to teams, colleagues and clients."

Government 2020: A Journey into the Future of Government

Figure 1: The Enterprise Risk Management process cycle



Understand the Context: The ERM process should be grounded in the context of the organization's strategic goals, key performance imperatives, major initiatives, and other defining characteristics that create risks and value adding opportunities for the organization.

1 **Identify:** Identify and categorize risks that impact the achievement of strategic goals and objectives

2 **Assess:** Apply risk rating criteria to evaluate overall exposure to the identified risks

3 **Prioritize:** Determine the most critical risks

4 **Respond:** Develop response to accept, avoid, reduce, transfer, or eliminate risk

5 **Monitor:** Provide timely and revelant updates to leadership on risk information

The Risk Intelligent model

To manage strategic and operational disruptions with greater intelligence, many private sector organizations have implemented Enterprise Risk Management (ERM) programs. These programs have traditionally helped companies create and preserve value, in good times and bad, by applying innovative approaches to risk management. It is also encouraging to see many private sector organizations taking their ERM programs to a higher level by integration with strategic planning, crisis management, and business resiliency, and by implementing tools to better analyze data for new threats and risks.

Many federal agencies are beginning to follow suit. A growing number are developing and implementing ERM programs to realize the benefits of becoming more risk intelligent. These agencies strive for a better understanding of their risk environments and to make better risk-informed decisions. At the same time, the Office of Management and Budget (OMB) is actively pushing for federal agencies to adopt more rigorous risk management programs.

The drive toward ERM is meant to supplement and enhance existing internal controls, which is one solution for managing risk. By incorporating ERM into an overall risk management structure, a federal agency can achieve full-spectrum risk awareness and risk response planning that leads to more effective coordination and communication across various risk-management processes.

Managing risk in uncoordinated and isolated silos can lead to blind spots and unanticipated events that put the federal agency in a vulnerable position with congressional oversight bodies and program stakeholders. Not knowing about a risk or threat does not relieve leadership of their primary accountability for managing it.

Managing risk at the enterprise level takes on increasing urgency as federal agencies come to grips with a growing list of emerging threats:

- **The rise of cyber-attacks.** The 2014 Quadrennial Homeland Security Review found that "growing cyber threats are significantly increasing risks to critical infrastructure, to the greater US economy, and imperiling the information security of the federal government and private sector."[1] And, as Admiral Michael S. Rogers testified before the Senate Armed Services Committee earlier this year: "Unfriendly states, organized criminals, and even unaffiliated cyber actors are stealing American intellectual property and using cyber means for coercion."[2]

- **Evolving terrorist threats.** The Homeland Security Review pointed to the difficulties in threat preparation: "Terrorist threats are evolving and, while changing in shape, remain significant as attack planning and operations become more decentralized."[3]

- **Human capital challenges.** Federal agencies also face risk from the inside. Increasing human capital challenges are driven by workforce turnover, difficulty in recruiting and retaining top talent, and enforcing standards for the conduct of personnel. These developments imperil the ability of many federal agencies to effectively execute their missions and protect the integrity of their reputation.

More than ever, federal agencies need the ability to risk-inform strategic and operational decision-making. The challenge has been implementation and institutionalization of ERM programs.

A critical lesson for both private and public organizations is that, although it is simple enough to start an ERM program, it can be challenging to adapt it to an organization's culture, maintain it continuously through the whole ERM lifecycle, and keep it nimble to respond to changes in the risk environment.

Developing and advancing ERM capabilities

Federal agencies manage many types of risks each day, using numerous methodologies and frameworks. But these practices are not often consistently coordinated, or adhere to industry-leading risk-management practices. Nevertheless, no federal agency is new to the concept of risk management. That's great news, because it projects a strong basis for developing, implementing, and sustaining an ERM program for the long-term.

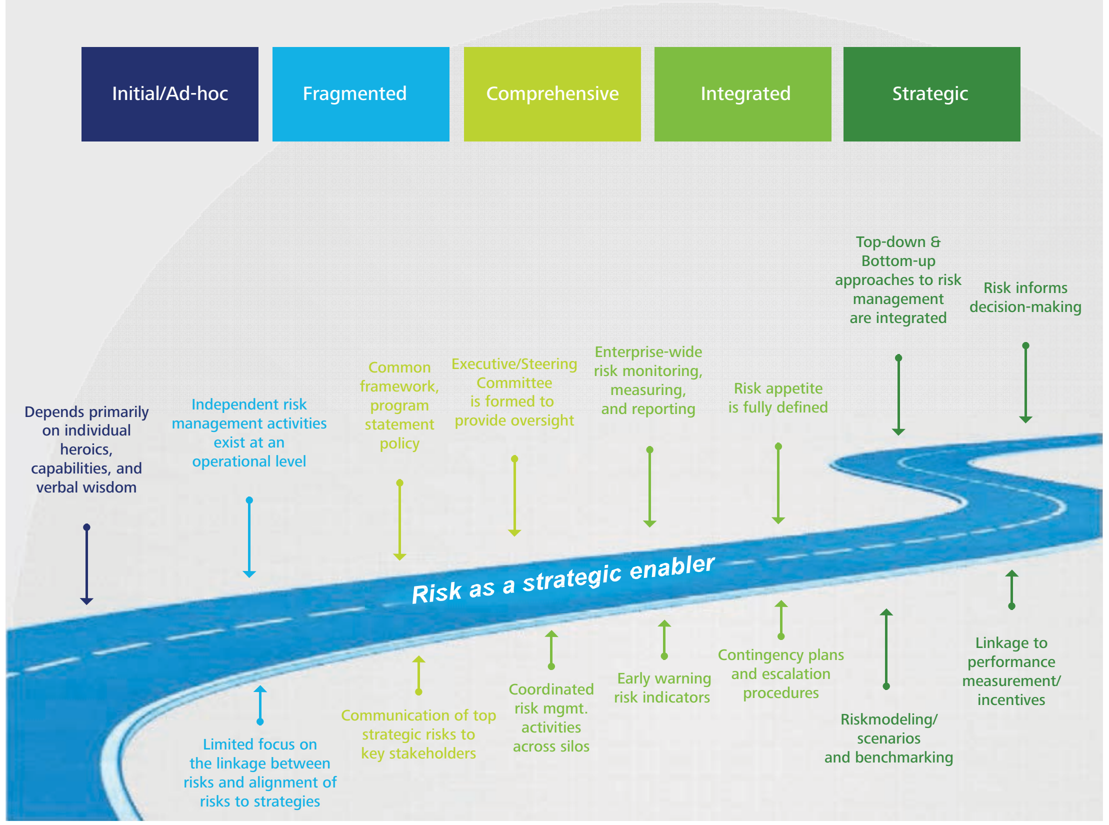
The question for federal agencies is how to move from what they have to what they need in terms of effective risk management at the enterprise level. There are no easy answers, but a good place to start is to acknowledge that producing an effective ERM program is a journey that takes time.

[1] The 2014 Quadrennial Homeland Security Review

[2] Statement of Admiral Michael S. Rogers, Commander United States Cyber Command before the Senate Committee on Armed Services. 19 March, 2015

[3] The 2014 Quadrennial Homeland Security Review

Figure 2: The Enterprise Risk Management journey


Initial/Ad-hoc
Fragmented
Comprehensive
Integrated
Strategic
Depends primarily on individual heroics, capabilities, and verbal wisdom
Independent risk management activities exist at an operational level
Common framework, program statement policy
Executive/Steering Committee is formed to provide oversight
Enterprise-wide risk monitoring, measuring, and reporting
Risk appetite is fully defined
Top-down & Bottom-up approaches to risk management are integrated
Risk informs decision-making
Risk as a strategic enabler
Limited focus on the linkage between risks and alignment of risks to strategies
Communication of top strategic risks to key stakeholders
Coordinated risk mgmt. activities across silos
Early warning risk indicators
Contingency plans and escalation procedures
Riskmodeling/ scenarios and benchmarking
Linkage to performance measurement/ incentives

This journey typically begins with existing ad-hoc risk management practices and culminates in risk-informed decision-making, and integrated top-down strategic and bottom-up operational approaches to ERM. *(See Figure 2).*

The journey toward an effective ERM program is measured in five stages:

- **Initial/ad-hoc.** Stage 1, characterized by a lack of formally defined processes and an ad-hoc, reactive approach to risk management largely driven by individuals.
- **Fragmented.** Stage 2, characterized by some formally defined processes and risk management activities. However, risk management activities are usually siloed, managed vertically within business units, and carried out independently. In general, risk management activities, risk information, and strategic decision-making processes are not aligned.
- **Comprehensive.** Stage 3, in which formal processes begin to emerge, initial tone from the top begins to drive integration of strategic risk management processes horizontally across the enterprise, and formal governance and management bodies are convened. At this stage, some siloed processes still remain, although knowledge is increasingly shared across functions and dedicated ERM resources are implemented.
- **Integrated.** Stage 4, with internal and external stakeholders now educated about risk management principles and practices. Activities are coordinated across siloes, and risk management escalation procedures are in place.
- **Strategic.** Stage 5, as top-down strategic risk information is integrated with bottom-up operational risk information at the enterprise level. Risk is used to inform strategic decision-making and planning at multiple levels within the organization. Early warning risk indicators are monitored and appropriately reported back to senior management. Finally, the organization takes an analytically rigorous approach to modeling risk.

The do's and don'ts of a strong ERM strategy

It's important for each agency to understand that ERM is not a turnkey solution to managing all risks. Instead, it should be viewed as a capability that enables a more informed understanding of the agency's risk environment, its evolution over time and future directions, and how the agency should undertake risk response to not only reduce risk, but promote better organizational agility and resilience.

> You can't predict every risk before it happens. However, you can take important steps to make sure that you're as prepared as possible to not only survive an unexpected enterprise risk event, but potentially capitalize on it in new and unexpected ways.

While there are many ERM success stories, there are also examples of ERM implementation failing to provide desired benefits. Common factors tend to show up consistently across enterprises, in attempting to determine how the program is set up, managed, and empowered:

- Lack of leadership buy-in for ERM.
- Cultural resistance to ERM throughout the organization, or at least in key quarters.
- Insufficient risk data or poorly performed data analysis (i.e., the data is available, but no one is meaningfully reviewing it).
- Persistent information siloes that stifle the full potential of an ERM program.

That's a blueprint for ERM failure. The characteristics of an effective federal agency ERM, to create future risk management value and sustainability, include:

- Leadership involvement and a sense of accountability.
- A defined vision for ERM within the agency.
- An objective understanding of where the agency stands, relative to its enterprise risk exposure.
- Agreement that change is needed, and that resources should be applied to make that change a reality.

These program pre-requisites are crucial, and demand an unbiased view of an agency's strengths and development areas as they relate to risk management. They require intensive review and discussion about whether the agency is fully prepared to do whatever is required to improve risk management capabilities in a dynamic operating environment.

The Deloitte Advisory difference

It isn't enough just to develop an ERM program. It should be done in a way that makes the organization able to survive and thrive in a dynamic risk environment.

Federal agencies should solicit help from those who've made the ERM journey before, can share important lessons learned, and draft innovative strategies to achieve the desired end result.

Developing a long-range plan with manageable phases of capability maturity, the agency can move intelligently along an implementation path, bringing the organization on board and generating early benefits.

This can place federal organizations in a strong position to effectively develop, implement, and sustain programs of their own, and realize the benefits of an effective ERM strategy.

These benefits include, but are not limited to:

- Reasonable confirmation of achieving agency objectives.
- A portfolio view of risk.
- Improved rewarded risk-taking and decision-making.
- Redeployment of existing resources as needed.
- A more timely and forward-looking view of emerging risk.

As used in this document, "Deloitte Advisory" means Deloitte & Touche LLP, which provides audit and enterprise risk services; Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. Deloitte Transactions and Business Analytics LLP is not a certified public accounting firm. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

That begs the question: What's next?

To enhance the opportunity for agency effectiveness, Deloitte Advisory recommends the following steps toward more proactive risk management:

- Define a senior leader vision for what ERM will look like when implemented well within the agency.
- Provide on-going ERM communication and training—from vision to application.
- Identify existing bottom-up or top-down risk management practices and processes already in place in each particular function or operational component.
- Design a custom-fit ERM framework that leverages, coordinates, and extends the agency's risk management capabilities.
- Draft an ERM implementation roadmap, and create an executive steering committee or other governing body to oversee ERM implementation and practice.

As the federal environment continues to shift in new and dynamic ways, the challenges in managing risk will only deepen, and require committed, innovative and effective responses.

The Deloitte Advisory view is that effective ERM is a requirement to building high-caliber strategies and capabilities to provide the services expected by the public—and for agencies to maintain the awareness, agility, and resilience to weather unpredictable operating environments. The public expects nothing less from its government.

Contacts

To find out more about developing your ERM program, contact:

Don Dixon
Director | Deloitte Advisory
Deloitte & Touche LLP
+1 919 546 8112
dodixon@deloitte.com

Patchin Curtis
Director | Deloitte Advisory
Deloitte & Touche LLP
+1 571 814 6071
patcurtis@deloitte.com

Folake Fadayomi
Senior Manager | Deloitte Advisory
Deloitte & Touche LLP
+1 571 882 8108
ffadayomi@deloitte.com

Anthony Fratta
Specialist Leader | Deloitte Advisory
Deloitte & Touche LLP
+1 703 915 9952
afratta@deloitte.com

This document contains general information only and Deloitte Advisory is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte Advisory shall not be responsible for any loss sustained by any person who relies on this document.