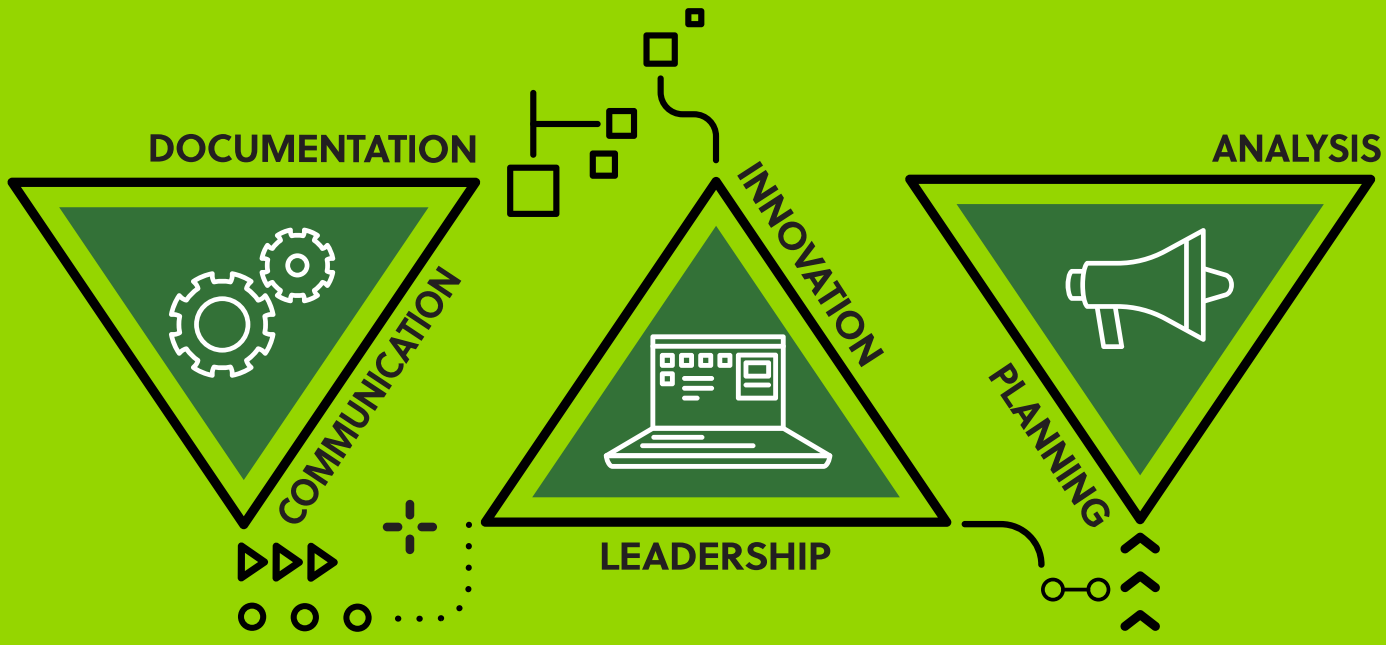


RESEARCH SERIES

An Agency Guide for ERM Implementation

AGA®

Corporate Partner Advisory Group
Report No. 39 | February 2017

Acknowledgements

Researcher & Author:

Thomas H. Stanton, JD teaches at Johns Hopkins University. He is a Past President of the Association for Federal Enterprise Risk Management and a former member of the federal Senior Executive Service. He is a Fellow and former board member of the National Academy of Public Administration and formerly chaired the Academy's Standing Panel on Executive Organization and Management. With a career that spans the practical and the academic, Stanton's work has led to the creation of new federal offices and approaches to delivering public services more effectively.

Corporate Partner Advisory Group:

Carlos Otal, CPA, Chair

David Fitz, CGFM, CPA, Vice Chair

AGA:

Ann M. Ebberts, MS, PMP, Chief Executive Officer

Susan Fritzlen, Chief Operating Officer

Maryann Malesardi, Director of Communications

Elizabeth H. Barnette, Marketing & Communications Manager

Anna Schumann, Communications & Marketing Manager

AGA is proud to recognize our sponsor for their support of this study.

CLA is a professional services firm delivering integrated wealth advisory, outsourcing, and public accounting capabilities to help enhance our clients' enterprise value and assist them in growing and managing their related personal assets — from startup to succession and beyond. CLA's team of professionals are immersed in providing solutions and services to clients in Financial Management and Reporting, Information Technology, and Assurance services throughout the federal government. With more than 5,000 people in more than 100 U.S. locations, and a global affiliation, CLA brings a wide array of solutions to help clients in all markets, foreign and domestic. For more information visit CLAconnect.com. Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.

AGA is *the* member organization for government financial management professionals. We lead and encourage change that benefits our field and all citizens. Our networking events, professional certification, publications and ongoing education help members build their skills and advance their careers.

AGA's Corporate Partner Advisory Group is a network of public accounting firms, major system integrators, IT companies, management consulting firms, financial services organizations and education & training companies. These organizations all have long-term commitments to supporting the financial management community and choose to partner with and help AGA in its mission of advancing government accountability.

Table of Contents

Welcome to ERM!

Why ERM?

Following the private sector's lead, numerous government agencies are adopting enterprise risk management (ERM) as a decision-making tool to help keep risks and rewards in balance.

In its simplest form, ERM asks the question, "What risks could prevent our agency from achieving its mission and objectives?" This simple question shows why ERM is so powerful:

- ERM focuses on the big risks that can affect the mission. This focus helps managers avoid getting distracted by the myriad small risks that otherwise could absorb scarce time and management attention while big risks go unattended.
- ERM is enterprise-wide. ERM helps to surface important risks that may be hidden in one part of the agency or distributed across the agency so that only a deliberate process such as ERM can bring them to light.
- By raising major risks to the attention of agency decision makers, and then prioritizing them, an agency can allocate its scarce resources (funds, staffing, management attention) to deal with the most important risks first.
- ERM looks at major risks, including failure to seize opportunities as necessary to succeed in a constantly changing environment.

The Association for Federal Enterprise Risk Management (AFERM) defines ERM as "a discipline that addresses the full spectrum of an organization's risks, including challenges and opportunities, and integrates them into an enterprise-wide, strategically aligned portfolio view. ERM contributes to improved decision-making and supports the achievement of an organization's mission, goals and objectives."[1]

ERM allows an agency's leaders to see the range of risks, across the entire organization, that could affect achieving the agency's mission. Once they know the risks, they can design approaches that improve agency performance, by building on strengths and minimizing potential impact of major risks, which could slow them down. In government, it is often the unexpected blow-up that brings down an agency and its leadership; ERM is a way to reduce the chance of that kind of unexpected major event.

Another way to look at ERM is in terms of information flow. ERM embodies a set of processes that allows information about risks to flow to decision makers, up and down the hierarchy and across an agency's silos and stakeholders. To do this, the office of the chief risk officer (CRO), or other top risk official, conducts interviews and workshops throughout the organization, especially with field staff and also with key stakeholders. The CRO and associated staff then investigate identified risks to determine whether there are root causes. This connecting of the dots can help assess risks, for example, that exist in disparate parts of the organization and haven't been previously understood as being "major." In tracking down the cause of a small discrepancy in financial statements, an accountant may discover a major shortcoming; similarly, the CRO may be able to use small indicators to detect large risks.

Once risks have been identified, they must be prioritized. Many agencies designate their top management team as the risk management committee. The risk management committee serves in an advisory capacity to the agency head or chief operating officer (COO); its function is to grapple with the reality that agency resources are limited and to take an agency-wide view of risks rather than merely defending resources for their own silo. The chief financial officer (CFO) is a key part of the risk management committee because he or she will have an agency-wide view of resources that may be used to address high-priority risks while not shortchanging other high agency priorities. The risk management committee also determines how best to address major risks. Risks can be accepted, avoided (by changing the relevant operations or activities), reduced or shared. For the agency head or COO, often insights gained from the discussion are as important as the risk management committee's final recommendations. Once the agency head or COO decides how to address the major risks, the CRO is responsible for monitoring implementation and reporting back to the risk management committee.

ERM also helps leaders of sub-agency units to place into a broader context the existing risks within their organizations. While these unit heads may have processes and systems in place to detect certain kinds of risks, ERM can help them understand these risks from an agency-wide perspective — including better understanding of similar risks in other units, root causes of identified risks, and ways to assess whether risks are being kept within appropriate limits.

ERM helps address the reality that the risks you anticipate may not be those that cause the most harm. One large regional financial institution, for example, avoided losses from subprime mortgages in the financial crisis, but was hit by a cyber-attack. To compound the issue, a rainstorm and flood wiped out key information systems located below ground level, in the basement. After dealing with the crises, the institution's chief executive officer (CEO) instituted a thorough ERM program so the company could address future vulnerabilities affecting its success.

The example illustrates how ERM is complementary to, but quite different from, the specialized kinds of risk management, (e.g., of credit risk or operational risk) in which organizations already engage. ERM is a method to survey the larger landscape, across the organization and its external environment and across the range of possible major risks, to determine the highest priority risks the organization and its leaders should address.

ERM helps overcome flawed decision-making. Sydney Finkelstein and colleagues at Dartmouth's Tuck School of Business found that bad decisions have two components: (1) an influential person such as a CEO or agency head makes an error of judgment because of, for example, misplaced reliance on a favored subordinate or a misperception that a current situation resembles one previously overcome. And (2) the organization lacks the right processes to bring facts to the table to challenge the flawed thinking and expose errors of judgment.[2] ERM, with its emphasis on bringing information about major risks to decision makers early, is a good way to help counter this problem.

Note the CRO does not manage or own risks; rather the CRO facilitates communication so information about major risks can flow to agency decision makers. Individual unit heads remain responsible for managing the risks in their silos. The CRO brings major risks to the attention of top management and other decision makers so an agency can help its managers deal with these risks before they get out of control. Just as important, the CRO can provide constructive challenge to a decision maker, such as when a new political appointee may not have considered the risks inherent in a major new initiative they enthusiastically support.

The facilitative, advisory and constructive challenge roles of the CRO and risk management committee are key to success; rather than exercising direct authority, they help the agency's top management identify, understand and address major risks. This helps prevent creation of yet another layer of bureaucracy within an agency; the purpose of ERM is to improve agency performance, not to impede action.

> The purpose of ERM is to improve agency performance, not to impede action.
>
> ‹‹‹

Too often, agency officials and civil servants are afraid to take risks. ERM helps by bringing to agency attention the danger of inaction. Standing still while the environment changes can be a major risk, and may prevent agencies from taking advantage of opportunities with a relatively small amount of risk but potentially significant rewards. Agencies striving to innovate and improve conditions need to take on some risk. Once an agency gains confidence from knowing the landscape, it is easier to move forward.[3]

One of the clearest metaphors about the value of risk management — and by extension ERM — in enhancing performance comes from the Financial Crisis Inquiry Commission interview with John Reed, former CEO of Citicorp:

> *"Why does a car have brakes? A car has brakes so it can go fast. If you got into a car and you knew there were no brakes, you'd creep around very slowly. But if you have brakes, you feel quite comfortable going 65 miles an hour down the street. The same is true of [risk] limits."*

Unknown major risks can cause the most damage. Once agency leaders set a risk appetite and the associated risk limits for each objective, the agency can increase its performance by avoiding obstacles ERM helps identify.

A Test of ERM — the Financial Crisis

The best demonstration of the value of encouraging flow of information about risks came from the private sector during the financial crisis. A study of a dozen financial firms, eight that failed or required bailouts after the crisis and four that successfully navigated the crisis, shows information flow — and leaders' openness to consider information about major risks — to be major determining factors.[4] Consider these two examples:

1. The retail banking side of JPMorgan Chase reported that a growing number of consumers failed to make their mortgage payments on time. Reported up the chain, this became a source of deliberation for the firm's operating committee. Investigation revealed the problem was widespread across the subprime mortgage market. The CEO instructed the firm's investment banking unit to sell all its subprime mortgages, well before the financial crisis began and well before many other firms learned of the toxic nature of subprime mortgages.
2. At another successful firm, Goldman Sachs, the mortgage unit lost money for 10 days when the firm's financial models had predicted they should have made money. Similarly, information flowed to the top of the firm, top management investigated and instructed the company to mitigate risk by hedging the mortgage holdings.

The two firms emerged from the financial crisis stronger than before, even while many other firms (including Lehman, Bear Stearns, Wachovia and Merrill) failed, had to be acquired or required a federal bailout.[5]

The financial crisis provides important lessons for ERM:

1. There are warning signs. Most risks don't suddenly erupt; rather, there are warning signs that — if people are looking — could tip off management in time to prevent serious harm.
2. Investigating is less costly than ignoring warning signs. Not all warnings are correct. Sometimes people mistakenly see major risks when there are none. Nonetheless, it is less expensive to investigate all warning signs, disregarding those mistaken, than to ignore a warning and hope everything turns out well.
3. Constructive challenge and dialogue can illuminate risk-reward tradeoffs. Once there is a warning sign, or if a regular review identifies major risk, then constructive deliberation is needed to determine whether the rewards are worth the risks or whether there is a solution that provides for a reasonable risk-reward tradeoff. The key to constructive challenge and dialogue is mutual respect; neither the person warning about risks nor the person pressing to move forward anyway is always right. Each must hear the other for a positive outcome, often superior to what either could come up with alone, to emerge.[6]
4. Information flow is essential, up and down the hierarchy, and across business units and support functions, and even with third parties such as contractors and program constituents. This means top management must set a tone of welcoming information and insisting on prompt reporting of risks to agency decision makers, the CRO, and the risk management committee. Reporting concerns should become the way the organization does business, rather than an act of personal courage.

> Reporting concerns should become the way the organization does business, rather than an act of personal courage.
>
> ‹‹‹

The Need for This Guide

We seek to provide a guide for government agency managers who would like to learn more about ERM, and how it can help agencies perform better and reduce chances that an unknown major risk within the organization could erupt with serious negative consequences for the entire agency and its reputation. Readers should also consult some of the documents referenced within and listed at the end of this report in **Appendix A**, especially the *ERM Playbook* created under the auspices of the Chief Financial Officers Council and Performance Improvement Council of the federal government.

ERM is a new and evolving approach to risk management, both for the private sector[7] and, now, for government agencies — at the federal, state and local levels. On the one hand, this creates opportunity for agencies to experiment with adapting ERM to their mission and circumstances; on the other hand, agencies need to apply the essence of ERM to help protect themselves against major risks that — if they materialize — can harm the function and reputation of the agency and its leaders and managers. This guide is written with that combination of flexibility and a firm conceptual structure in mind.

In recent years, federal government departments and agencies have experienced major problems stemming from undiscovered risks. Organizations such as the U.S. Department of Veterans Affairs (with respect to VA hospitals), the Internal Revenue Service (screening politically active exempt organizations), the General Services Administration (a lavish conference), and the Office of Personnel Management (a major cyberattack), each show a pattern: an unattended-to major risk erupts, causing a reputational crisis — often in addition to actual harm — and a wave of firings, including the agency head or departmental secretary, occur. These are negative examples of agencies failing to practice effective ERM. There are positive examples, too, which this guide discusses, of ERM making the difference between success and failure at an agency.

ERM cannot identify all major risks nor always prevent major risks from causing harm; rather, ERM is a tool that — when well implemented — can substantially reduce the chances of major harm occurring. ◁

Adding ERM to Agency Processes

Introducing ERM

The secret of ERM is that, unlike other agency processes, one cannot simply direct people to accept ERM. A requirement to adopt ERM would turn it into a compliance exercise rather than an actual contribution to agency decision-making. Telling agency personnel to report risks to top management simply doesn't work if people are fearful of retribution or otherwise don't want, or feel they have the time, to do it. Ultimately, the agency's culture needs to embrace ERM if it is to work. Because there is a good case to be made for ERM, a more effective approach is to discuss it with agency leaders and managers before installing a CRO or risk management committee. As increasing numbers of federal agencies adopt ERM and advance its implementation, there will be increasing numbers of examples of how to make ERM work under various circumstances.

Early federal government adopters of ERM, including the U.S. Department of the Treasury, have decided to prepare their organizations even before a CRO is hired. At one agency, the agency head convened political officials and career senior executives for a roundtable discussion. Participants identified risks they thought were highest. Then, officials heard a presentation by a federal ERM specialist (not a candidate for the CRO position) and engaged in a question-and-answer discussion.

A requirement to adopt ERM would turn it into a compliance exercise rather than an actual contribution to agency decision-making.

The ERM specialist followed this up with meetings with key executives and managers to discuss their risk concerns off the record. The agency arranged a series of brown-bag lunches to hear from CROs at federal agencies with strong track records of success. As familiarity with ERM grew and trust built, the quality of give-and-take at these meetings improved.

Several lessons emerged. First, there must be ground rules. Most importantly, blame is inappropriate; agency officials need to see themselves as part of the same team so the people in units where perceived risks might be greatest — often in support areas such as personnel and IT — are free to join in the effort to identify risks and deliberate about ways to address them. If the group pummels people "responsible" for risks, then people —often those who know the most about possible solutions — would simply keep quiet. Thus, in addition to analytical skills, a CRO must have facilitation skills to maintain a constructive tone throughout the risk-identification process, even if participants show passion because of genuine needs and concerns.

Second, the process needs to engender trust. Interviews and workshops, specifically structured discussions with selected groups of managers in key parts of the organization, need to maintain a constructive tone. If an issue requires urgent attention, discussion determines how best to raise it with trusted agency leaders. It is important no one be "burned" for raising candid concerns. Also, the official in charge of a business unit in which a major risk might be found, must be confident the result will be constructive attention rather than blame.

If the group pummels people "responsible" for risks, then people — often those who know the most about possible solutions — would simply keep quiet.

Third, the process of introducing ERM works best when it cascades downward, from the agency leadership to top managers to agency managers. The tone throughout the process should be: top management wants to adopt ERM for the agency, here's why we think it has value, here are tentative plans how we might build the risk function into the agency's organization, and please give us your feedback while we're still in the design phase.

On July 15, 2016, the Office of Management and Budget (OMB), in its release of the updated Circular No. A-123 *Management's Responsibility for Enterprise Risk Management and Internal Control* (Circular A-123) signaled that agencies are encouraged to implement ERM; the idea is to stress this is not simply a compliance exercise, but rather, a way to advance the agency's prospects and avoid harm from serious risks.

Preconditions for Making ERM a Success

Perhaps the most important precondition for ERM to succeed is top leaders must see value in ERM and want it to succeed. There are several reasons why "tone at the top" is so important. First, many agencies find themselves with growing workloads but diminishing budget and staffing resources. Agency managers, and especially agency senior executives, are busy. Top leadership support is needed to persuade them to set aside the day's pressing demands and discuss ERM. Many executives believe they already have identified and managed their major risks, and many times they are right. It takes support from the top, and a trusting relationship, before executives will share this important information in an ERM process they may not control.

Second, support from the top encourages executives to engage in constructive dialogue, rather than taking defensive action to thwart investigation of major risks in their areas of responsibility. Top leadership can encourage constructive dialogue by stressing that the point of the exercise is not blame, but rather to determine where scarce agency resources might be allocated to deal with the most significant risks. In other words, executives who report their most pressing risks sometimes may benefit from a needed increase in resources to deal with them. Top leaders need to create an environment in which feedback is heard and responded to appropriately.

Third, support from the top must protect the risk function. Some parts of the agency may be more willing to collaborate in the ERM process than others. If one part of an agency refuses to give the CRO's office access to conduct interviews about major risks, for example, that would be a major warning sign. The agency head cannot afford to be uninformed about possible major risks in part of the organization, especially one that refuses to discuss risk. The agency head — whose own reputation, as well as the reputation of the organization, is at stake — has authority to intervene to protect the integrity of the ERM process. The agency head can intervene directly or through the COO to ensure risk information flows properly to the decision makers. How and when to address such issues must be determined.

Finally, and probably most important, the agency head is essential to ensuring that, when important risk information surfaces, the agency takes the necessary steps to address major risks. ERM turns into merely a gesture if it operates to identify, analyze and prioritize major risks that are then left unaddressed. Only top leadership can ensure a proper response and the allocation of resources needed to respond effectively. Absent effective leadership from the top, it's best for subordinate unit heads to practice ERM within their own organizations, and wait until a debacle occurs and the agency comes to realize ERM can help the agency, or until the agency head is replaced with new, better leadership.

The agency's management team is also critical to success. Good management prescribes that the agency head and COO work to coalesce the agency's top managers into a mutually supportive management team that considers what's best for the entire organization rather than merely for their unit. An agency head could consider top managers simply protecting their own turf a warning sign.

Locating the ERM Function in an Agency

Especially at the beginning, when ERM is new to an agency, the ERM function should report directly to the top of the agency. Otherwise, the risk function can be swallowed up by prevailing bureaucratic forces. On the one hand, the CRO needs to be able to speak with confidence that backing from the top leadership is in place. On the other hand, the CRO needs to possess interpersonal skills so people throughout the organization trust they will not suffer adverse consequences from sharing risk information.

In many organizations, the office of the CFO (OCFO) can serve as a useful incubator for establishing the risk function. The CFO tends to be positioned to see disparity between available resources and agency needs. The risk perspective can be an important tool for making decisions about what should be funded or where resources can be reallocated to address risk. Perhaps most importantly, the CFO is positioned to take the kind of agency-wide view that a CRO must take at the start of ERM development.

While the OCFO may be a good place to incubate the CRO function, effective application of ERM requires different skills than those of the typical CFO. CFO and CRO responsibilities are quite different. Whereas the CFO takes a view largely of the agency's internal operations, and, for example, applies and administers internal controls, the CRO must take a broader view that includes assessment of external as well as internal risks, and that considers internal controls to be part of a potentially flexible risk response rather than as a set of fixed compliance requirements. Although helpful in the initial stages of ERM implementation, the CFO function and its demanding timetables and requirements can displace the more fluid CRO functions that must be carried out for ERM. Accordingly, it is best if the CRO function is ultimately separated from the OCFO and reports directly to the agency head rather than be layered under the CFO function. Thus, when the agency head is ready, the ERM function will work most effectively if it is separated from the CFO's office.

Another question relates to the extent that the ERM function might be combined with responsibility for project or program management within an agency. The Institute of Internal Auditors (IIA) developed a concept of the "Three Lines of Defense." It is helpful to recognize that, while ERM can aid in reducing the risk and increasing the range of potential positive outcomes of program and project management, risk management (and ERM in particular) is most effective when it operates separately from direct operational management. As the IIA explains:

> *"The Three Lines of Defense model distinguishes among three groups (or lines) involved in effective risk management:*
>
> - *Functions that own and manage risks.*
> - *Functions that oversee risks.*
> - *Functions that provide independent assurance.*
>
> *"As the first line of defense, operational managers own and manage risks. They also are responsible for implementing corrective actions to address process and control deficiencies…*

"In a perfect world, perhaps only one line of defense would be needed to assure effective risk management. In the real world, however, a single line of defense often can prove inadequate. Management establishes various risk management and compliance functions to help build and/or monitor the first line-of-defense controls." [8]

Thus, project management and program management are kept distinct and separate from the ERM function in an agency. As the first line of defense, project and program managers own their risks and assist in risk identification; but it is the second line of defense, usually including a CRO and a risk management committee that implements ERM across the agency.

Deciding about a CRO and a Risk Management Committee

The risk management function needs to be managed by a high-level executive, preferably a career senior executive — to ensure continuity over political transitions — who focuses explicitly on risk. An agency can take steps toward ERM without designating a full-time CRO. The key components are (1) a top-level champion for ERM at the agency; (2) a knowledgeable senior official, often the CFO, to begin the process of identifying major risks and convening a high-level working group to discuss how to deal with them; and (3) a strategy for developing ERM through a series of incremental steps to allow ERM processes increasingly to permeate how the organization does business.

At some point, as the ERM function matures, it will be necessary to designate a CRO to lead the effort. The CRO provides an administrative focus for implementing ERM, with special attention to identifying and assessing major risks and their root causes. However, ERM implementation should be a group effort. Even with top backing, one individual is unlikely to be able to provide the leadership and carry out the activities needed to make ERM a success. The interagency *ERM Playbook*, which avoids taking a stand for or against designating a CRO, does warn that a CRO cannot become effective at most mid- or large-size agencies unless supported by staff. Also, to enable the CRO to operate at the senior executive service (SES) level within the federal government, the CRO must direct at least some staff, although the size depends on the agency and its resources and needs.

The risk management committee, supported by the CRO, is another essential element of ERM, whether formally called a risk management committee or not. This group, which should consist of senior-level, well-respected officials, often at SES rank, helps drive ERM at the agency. The risk management committee is responsible for advising the agency head or COO on the priority of major risks that need to be addressed. Many agencies will find that their operating committees, composed of top management, can simply add risk to their scope of responsibilities and serve as the agency's risk management committee. Other agencies may find it best to create a risk management committee comprising senior managers most inclined to take an agency-wide view of risks, and who can raise constructive challenge and deliberate about agency-wide tradeoffs without being unduly prejudiced toward the part of the agency for which they are responsible. The way the committee functions may depend on the leadership style of the agency head or COO.

> ERM cannot protect against all risks that may materialize; rather it is a useful approach to reduce an agency's exposure to risks that could cause harm.

Attributes and Role of the CRO

The CRO does not manage risk; rather, the CRO is a facilitator whose office conducts interviews and workshops across the agency and possibly with stakeholders and other third parties. The CRO should seek to build trust across the agency so people become comfortable reporting what they perceive to be major risks. Bringing "bad news" to the top, so it can be appropriately addressed, becomes the way the agency does business.

In most cases, this means the CRO is an agent of cultural change, creating an atmosphere in which people understand they are all on the same team focusing on improving agency performance by identifying, assessing, prioritizing and addressing major risks — before serious harm materializes. The CRO must articulate and demonstrate the value of ERM to agency leaders and managers. In a world of constant media exposure, the CRO's work is essential to protect the agency from unanticipated mishaps that can harm the agency's performance and reputation — and perhaps trigger repercussions that affect everyone, whether they had been responsible for that part of the agency or not. That said, ERM cannot protect against all risks that may materialize; rather it is a useful approach to reduce an agency's exposure to risks that could cause harm.

The CRO needs to become familiar with the agency and its workings. Formerly, it might be that the powerful head of a business unit could simply stonewall efforts to identify major risks. Today, with evidence of too many failures of risk management by government agencies, it has become clear everyone in the agency has a major stake in ensuring the success of ERM and in identifying major risks early.

The CRO is an advisor to the agency head and COO about risks and how to address them. The CRO staffs, and generally chairs, the agency risk management committee and helps the committee understand the root causes of identified risks and then prioritize them based on perceived likelihood and severity. With leadership from the CRO, the risk management committee may need to provide constructive challenge to the agency's decision makers, to introduce possibly divergent points of view to help resolve major issues.

The CRO may also work with the CFO and other agency leaders to determine resources available to address major risks. Once the agency head determines which risks to address and how, the head of the unit in which the risk resides is tasked with implementing the selected risk-management approach. This is key, because the unit head has both the resources and knowledge needed to make risk management effective. Based on milestones for addressing a risk, the CRO monitors the process of implementing risk management and reports progress to the risk management committee. Since risk management is an iterative process, the CRO informs the risk management

committee of lessons learned from managing one set of identified risks so other risks may be better identified, analyzed and addressed.

The CRO brings considerable substantive knowledge; for instance, in advising the risk management committee, the CRO may point to the problem of risk velocity and the likely amount of time available to the agency to address an identified issue. Once an agency gains experience with ERM, the CRO can help the risk management committee and agency head determine the agency's and activities' risk appetite. Risk appetite specifies the amount of risk an agency wants to take in a specific area. Many agencies have a statutory mission to take on risks the private sector might consider excessive, such as in extending credit for lower-income households or untested new business ventures. The purpose of a risk appetite statement is to help an agency achieve balance between risks and achievement of mission. To further use a federal loan program as an example, an agency must take more risk than a private lender might, but must limit its risk exposure to prevent an unacceptable, or unbudgeted, volume of loss. One major purpose of a risk appetite statement is that it makes clear risk-taking is inherent in achievement of an agency's mission. For some agencies, or some agency activities, the risk appetite statement will call for reduced risk-taking; whereas for others, increased risk-taking may be in order.

Staffing Considerations

Most federal agencies find themselves constrained for resources. That means the CRO office, especially before it has demonstrated its value to executives across the agency, may need to begin operations with a small staff. The key is to staff the office with a team that combines knowledge of the agency with ability to provide the facilitation and analytical services required to implement ERM, and show value to the organization.

Anette Mikes, formerly of the Harvard Business School, has done considerable work on ERM in the private sector. She reports on a highly successful ERM office that functions well with only three people (three personality types):

> *"The first one is someone to make it happen. That's me. Okay, somebody who will push down doors, is driven, and has the credibility and authority to open doors and make it happen. The second is a nice charismatic personality who people enjoy working with. And that was [the Workshop Facilitator], an absolute charmer. A super nice guy … very knowledgeable, who became a very good [workshop] facilitator. The third one is a person with an analytical mind who can manage the vast quantities of data [collected at the workshops]. You don't find those characteristics in the same person, so I teamed them together."* [9]

Especially at the beginning, the CRO may need access to contract staff to support the office and its responsibilities. An experienced contractor can help while a new CRO seeks to determine which tools to apply to implement ERM at the agency. Selecting contractor support requires considerable care, especially as contract funds may be limited. Contract staff can offset government staff ceiling levels, and can add needed skills, especially at the start of the process. CROs should stay away from large amorphous teams and focus instead on contractors with a demonstrated track record. Contracted staff can also help to train and transfer knowledge to existing government staff.

Role and Composition of the Risk Management Committee

Generally chaired by the CRO, the risk management committee advises the agency head and COO. Its primary task is to review and assess risks identified, and help prioritize them. The committee then considers ways to address the highest priority risks and allocate scarce agency resources (e.g. funds, staffing and management attention) to deal with them. The committee has no independent power; rather, it is a deliberative body that helps the agency head weigh risks and rewards of alternative courses of action. The risk management committee also helps the agency head and CRO adopt an annual plan for implementing ERM and monitors progress in achieving the milestones of that plan.

Members of the risk management committee should be senior in rank, drawn from across the agency and its functions, collaborative in approach, ready to provide constructive challenge, and selected for their willingness to consider an agency-wide view rather than merely the perspective of their own organizational silo. It should include respected members from field offices, not just officials located at agency headquarters. As too many agencies have learned, major risks can reside in the field, unrecognized; appointing diverse senior people helps address this and integrate the ERM process with field operations.

Often the agency's top management committee, such as an operating committee, can also serve as the risk management committee. In such cases, it is good to separate meetings on risk management, to ensure an inordinate amount of time is not spent on operational risks rather than other possibly more major risks that agency decision makers need to address. An indication of the separation can be that the CRO chairs and staffs the risk management committee. While the CRO may lead discussions that include more senior officials of the agency, the constructive role of the CRO and advisory role of the risk management committee make this possible and productive.

Regarding the size of the risk management committee, a group of up to eight senior people can foster robust discussion. Inevitably, some units will be left out; it is up to the CRO to ensure that people across the agency have been interviewed and that risks from both large and small programs are included in the committee's deliberations. Again, the committee's perspective needs to be that the highest priority risks be identified, analyzed and addressed, regardless of where they reside. ◁

Establishing the ERM Function

The U.S. Bureau of the Census, which has established one of the more effective ERM programs in government, suggests seven steps for implementing ERM:

1. establish tone at the top;
2. develop an ERM strategy, including an ERM framework and plan;
3. identify roles and responsibilities;
4. build processes and capabilities;
5. implement processes and capabilities;
6. increase awareness and conduct training; and
7. assess and increase maturity of processes and capabilities.[10]

Agencies, their leaders and CROs will want to chart a course that includes these seven steps in a form and sequence that best suits their circumstances. The following discussion points are intended to be suggestive about considerations agencies need to keep in mind as they roll out and strengthen their ERM programs. Internal circumstances, considerations of stakeholder interests and external context should shape each agency's approach to implementing ERM.

When establishing ERM, consider these questions:

- To what extent does top agency leadership support implementation of ERM?
- To what extent do the agency's business unit heads consider themselves an integrated management team concerned about risks to the entire agency rather than just focusing on risks to their individual units?
- Where can constituencies to support ERM be built and strengthened?
- What are the major risks facing the agency? How urgent is it to address them?
- How can ERM show its value early to agency leaders and stakeholders?

> Which group of people will deliberate most thoughtfully, best help prioritize risks and, generally, provide the most useful advice about major risks the agency faces?
>
> ›››

Establishing the CRO Position: First 90 Days

Once the agency head or COO decides to establish the ERM function, the idea needs to be deliberated with top managers. Even those managers not yet convinced of the value may have constructive ideas about fitting the CRO position and function into the agency. Once the agency head decides where to situate the CRO function, agency hiring processes come into play, including writing the personnel description, posting the position, and hiring the CRO. The *ERM Playbook* contains several personnel descriptions to consider, and others also are freely available from agencies that already have hired CROs.

The agency head also needs to consider the most suitable framework for the risk management committee. Sometimes there is a tradeoff between including the most powerful unit heads and including those most open to considering risk from an agency-wide perspective. As with any management decision, the agency head may wish to begin with one set of members for the risk management committee and then adjust as experience suggests. The touchstone question: Which group of people will deliberate most thoughtfully, best help prioritize risks and, generally, provide the most useful advice about major risks the agency faces?

Even before the CRO comes on board, it is important to establish a constituency in support of ERM. Groups tend to go through three stages:

1. inclusion, when a new person joins an established group, and needs to gain acceptance as a member of the group;
2. control, when established members of the group need to accustom themselves to responding to suggestions and recommendations of the new person; and
3. affection, when the new person is accepted as a member of the group in good standing whose recommendations or decisions are likely to be accepted.

Preparing the agency before a CRO comes on board can help reduce friction as the CRO goes through these stages.

The most important responsibility of the new CRO is to establish trust. The second most important action, to learn how the

agency works; who has influence and whose judgment is questioned; and the informal as well as formal details of how different kinds of decisions are made. The CRO will need to leverage agency-head support to meet with senior officials to explain ERM and its value. These meetings can help surface concerns about the risk function and areas in which the CRO may need to accommodate processes and approaches to take account of key issues. The purpose of these meetings, by demonstrating openness to constructive dialogue about the risk function, is to build a constituency in support of what the agency head is trying to accomplish by establishing ERM in the organization.

While the conversations are taking place, the agency head can convene the risk management committee to develop the framework for unfolding ERM in the agency and to build working relationships between the CRO and risk management committee. Important aspects of the ERM framework include (1) a charter for the risk management committee; (2) a work plan for identifying, analyzing and prioritizing major risks; (3) ways to integrate risk considerations (and the CRO) into key agency process such as budgeting, strategic planning and training; and (3) a table of deliverables and timetable for delivery.

Product deliverables can include internal requirements such as creating a risk register and other helpful tools; an ERM policy statement that sets forth responsibilities of the CRO, the risk management committee, unit heads and agency officials with respect to ERM; and a long-term maturity model that sets forth stages of development of ERM at the agency (see **Figure 1**). The *ERM Playbook* contains useful models and templates.

Other deliverables may be externally mandated, most notably the annual agency risk profile called for by Circular A-123.

The CRO also will want to address groups of agency officials, perhaps as a segment of regularly scheduled meetings or training sessions. And, as sketched in the discussion of preparatory actions, above, the CRO may want to offer brown-bag lunches or other informal meetings at which CROs from other agencies speak and share their experiences with ERM.

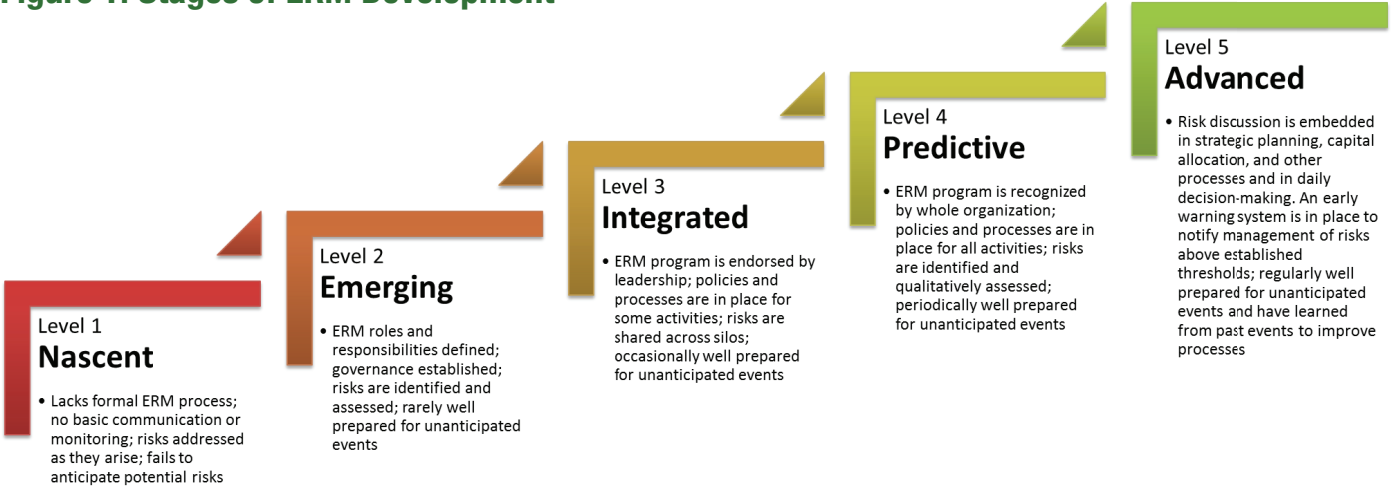
During these meetings, it will be important for the CRO to reassure agency officials that (1) ERM will not displace risk management functions in which they already engage; (2) ERM is a minimally disruptive process that seeks only to identify and deal with large risks that the agency leadership and other agency decision makers need to know about; (3) identification of high-priority risks is a problem-solving rather than a potentially punitive exercise and (4) identification of major risks could result in allocation of additional resources to address them. Moreover, the risk management committee does not create another level of bureaucracy; while it may engage in constructive challenge concerning major risks, is solely advisory in its mandate.

One particularly important meeting should be with the agency inspector general (IG). Both the agency risk management (ERM) function and the IG are responsible for detecting major risks before they cause harm, and both are likely to face resource constraints compared to the broad scope of their responsibilities. Yet the roles are different: the CRO is a part of the agency's senior management, whereas the IG must operate with independence to, if necessary, present a negative report about the agency leadership.

The CRO and IG should develop a sound working relationship that enhances the value provided by each role. One consideration at the core of that working relationship: no one will report information about major risks to the CRO if they think it will become fodder for a critical IG report. The degree to which the CRO can build a relationship of trust with agency leaders and staff, and the extent that the IG can respect and avoid disrupting this trust, are paramount to success of the ERM program. Without trust, communication — so essential to making ERM a useful reality — may be stifled.

Somehow the CRO and IG need to build a relationship that encourages reporting of major risks. Ideally, a constructive resolution might be that the IG, in reviewing agency vulnerabilities, gives the agency appropriate credit for major risks identified and being addressed. Conversely, if the IG identifies a major risk that the ERM process has not surfaced, then that would seem to be fair game for a critical report. The IG can play an important, independent role in assessing and reporting on the quality of the agency's risk management and ERM implementation.

Figure 1: Stages of ERM Development



Source: *ERM Playbook*

The risk management function may gain the reputation of a dispassionate defender of the best larger interests of the agency, and its challenges and opportunities.

Establishing the CRO Position: Follow-Through

As the CRO conducts interviews with individuals and groups across the agency, major risks may become apparent. At this stage, root-cause analysis (RCA), which enables the CRO to systematically analyze the cause-and-effect relationships of an event or situation, may be appropriate. Using RCA, the CRO identifies ways to stop negative events reoccurring, while examining successful events to help replicate their positive characteristics. The CRO may want to consult seasoned people within the agency to determine whether others have seen the risks, how and why they arose, and why they haven't been addressed. From these consultations, the CRO may develop a short list of possible "quick wins" to present to the risk management committee. For instance, before a change of presidential administration, the CRO and risk management committee may want to develop a major risk report for the incoming political leadership, highlighting major risks and opportunities, and ways of addressing the greatest risks. With this approach, the risk management function may gain the reputation of a dispassionate defender of the best larger interests of the agency, and its challenges and opportunities. In some agencies, unit heads are likely to point to personnel and information technology issues as causes of major risks. Sometimes, these issues become sources of controversy. In such cases, a quick win might be to have the risk management committee propose commissioning an independent management review of such an area of risk and controversy, to defuse blame and determine constructive approaches for addressing the largest risks.

There is a range of possible "quick win" deliverables the CRO can provide. At one agency, it was discovered that managers were submitting large volumes of reports no one was using or even reading. Investigation revealed that these high-priority "Commissioner's Reports" had accreted over time, as each new agency head requested reports on different topics. By surveying top managers, the CRO could show that many of these reports could be eliminated, thereby reducing burdens on management and making it more likely that information in the remaining reports be read and used.

At another agency that had adopted ERM after a major risk caused substantial reputational and other harm, the new CRO found operations of a comparable unit in which major risks had materialized, and flagged the risk before it became public. By analyzing the problem, the CRO suggested process adjustments that allowed for resources to be reallocated and solved the problem.

With a robust picture of risks across the agency, the CRO can apply an increasing number of tools, including heat maps, dashboard indicators, and an ERM tool that develops standardized risk reports and can generate standardized, forward-looking reports on types of risk and their likely incidence and severity across the agency. These tools can become essential when the scope of the risk identification and analysis processes becomes so large that tools are needed to track the status of major risks, and decisions the risk management committee and agency leadership make about whether and how to address them. Each tool should facilitate the flow of risk information and prioritization.

As the CRO seeks to establish the ERM function, a dilemma may emerge. On the one hand, starting with quick wins and seeking incremental gains can show an agency the value of ERM. On the other hand, a CRO must not become relegated to a superficial role, such as a mere commentator on agency processes and procedures, without ability to identify major risks and obtain a response from the agency's leadership. The answer to the dilemma is to build on support from the agency leadership to integrate ERM as a basic element of regular agency processes such as strategic planning, budgeting and general decision-making. Consider each of these, in turn, and how ERM can add value.

Strategic Planning: Because ERM seeks to identify and deal with risks that could prevent an agency from achieving its mission and objectives, a major benefit of implementing ERM is its effect of leading agencies to focus on a clearer statement of objectives. While an agency's mission statement may be diffuse and general, its goals and objectives are intended to be specific, measurable, time-related and realistic so one can determine whether they have been achieved on time. By asking if there are risks that can prevent achievement of objectives, ERM can lead agencies to specify what they are trying to achieve, by when, and to what extent. Once objectives have been honed, ERM can help agency leaders better understand external threats and opportunities and internal capabilities, and assess the agency's strategy and objectives in terms of risks and rewards.

Budgeting: Federal agencies, especially those whose activities depend on discretionary appropriations, face continuing budget pressures. Here, ERM and the emphasis on conversations and prioritization become critical. The operative question for ERM at a time of budget constraints becomes: "As our agency refocuses its mission to operate with a significantly reduced budget, what are the major risks that could prevent us from accomplishing our mission and objectives?" This becomes an invitation for agencies to rethink their core missions and processes rather than blindly trying to do more with less.

In this context, agencies need to consider adopting risk-based budgeting, to help balance performance, risks and resources. Instead of the frequent practice of simply allocating cuts pro rata across activities, agencies will need to separate their activities into categories:

1. those prescribed by law or that otherwise are essential to carrying out the agency's core mission;
2. those that need to be maintained to sustain agency capabilities long term;
3. those of special value to important constituencies; and
4. those that would be valuable if funds are available.

Cuts then can be allocated to protect the first two categories, applying most cuts to the fourth, to the extent necessary and politically feasible.[11] In many cases, agencies will need to obtain clearance from OMB (or other appropriate agency organization) and the relevant appropriations subcommittees to obtain optimal benefits from this approach.

Decision-Making: Too often, agency leaders possess too little information to make a sound decision. This can happen when a business unit head proposes a course of action while other unit heads simply agree or acquiesce, possibly because they do not want to face disagreement in turn when they propose a decision. To improve the quality of decision-making, it then becomes reasonable, when a business unit proposes a new initiative or other significant decision, that those urging the decision also be called on to discuss major risks and how they have been addressed. When a leader routinely requests consideration of risks before making a major decision, this can prompt proponents of future proposed decisions to first investigate whether major risks exist in their proposals. The CRO then may suggest additional ways to address the risk or refer the decision about how to address possible risks to the risk management committee. In this way, ERM adds to the amount of relevant information available to the agency head and other decision makers before, rather than after, an important decision is made. The CRO also can provide statistical and other information to help persuade legislators to reduce the risks posed by proposed legislative initiatives, and especially by poorly structured efforts to reduce appropriations.[12]

ERM Tools and Approaches

The key consideration when adopting a tool or approach is to decide whether or to what extent it can be useful in assisting the agency to implement ERM. It is also important to remember that use of interactive processes to identify and prioritize risks and decide on cost-effective responses is the conceptual core of ERM; as two experts note, successful implementation of ERM is "something that cannot be achieved by filling out and auditing checklists or installing Governance, Risk, and Compliance (GRC) software."[13]

Interviews and Workshops

Interviews are essential to obtain information up and down the organization and across the hierarchy. Some information relates to major risks and ideas for cost-effective ways to address them. Other information provides feedback to the CRO about how the ERM function is perceived within the agency and how it might be made more attractive. Interviews also help the CRO find individuals who are especially capable, in favor of ERM, and willing to consider risks from an agency-wide perspective. Depending on the CRO's approach, it may be helpful to include these people in an ERM network to provide a source of timely information about particularly threatening or otherwise important risks and proposed ways of addressing them.

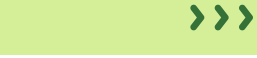
Workshops are interviews with groups of people — from one part or multiple parts of the agency. Workshops have a variety of benefits. A workshop with managers from two parts of the agency can help illuminate boundary issues between the two and how risks shift from one part to the other. Other workshops can consider scenario analyses, and managers' responses and feedback on the likelihood and severity of various risks and what might be done to respond. Some workshops involve a voting device so participants can anonymously rank possible risks and outcomes.[14]

Risk Register

After gathering information about risks from a multiplicity of sources, the CRO must bring order to the information. In developing the risk register document, the CRO records the risks identified according to priority. The risk register indicates the risk's nature and owner, and the plans and timetable for addressing it. The CRO adjusts the information as appropriate, such as if a risk increases or drops in priority, or if a risk management approach is successful. Since ERM focuses on major risks, it is important to limit the risk register to a manageable number — typically fewer than 20.

Risk registers can be used by managers at multiple levels within an agency, each rolling up to a higher level. The importance of ERM is to strengthen decision-making, and risk registers should maintain a coherence with that in mind. ERM seeks to focus on the risks that affect achievement of the agency's mission and objectives; that means the risk register should list only the most important risks to address or monitor whether they are trending in a negative direction.

ERM seeks to focus on the risks that affect achievement of the agency's mission and objectives; that means the risk register should list only the most important risks



Scenario Analysis

Financial institutions use scenario analysis (that some call "reverse stress-testing") to determine scenarios that could cause serious harm to the institution. Experience teaches that some scenarios are unlikely to unfold as envisioned; but the benefit of scenario analysis is to help decision makers see how the pieces fit together, how risks can concatenate across the organization, and the mission activities that are most likely to be affected. Scenario analysis is also helpful in determining which responses to risk might be the most effective.

Risk Indicators and Dashboards

Once a risk has been identified as major, decision-making can benefit from creation of one or more indicators for that risk. Tracking the relevant indicators can show the CRO, the risk management committee and decision makers how the risk is trending. Over time, an indicator can show developments in the amount of a specific major risk that the agency is accepting or managing. If an agency has developed a statement of risk appetite, then a risk indicator can be used to determine whether the risk exceeds the agency's risk limits or remains in bounds.

Ideally, risk indicators should be forward-looking to help anticipate future developments. Analysis can determine which factors play a significant role in causing particular risks and indicators can be found that reflect those factors. For instance, an agency may find that demand for its services can increase or decrease,

Figure 2: Heat Map

	Likelihood	Unlikely	Possible	Likely	Almost Certain
Impact	Description	The event could possibly occur, but is unlikely at this time.	The event could occur under specific conditions and some of those conditions are currently evidenced.	The event is most likely to occur in most circumstances.	The event is expected to occur in most circumstances or is happening now.
Catastrophic	Large unacceptable financial loss, severe budget variance. Very significant harm to image with substantial impact on effectiveness. Large and unacceptable operational impact, long term business interruption. Qualified audit finding.				
Major	Very significant financial loss, major budget variance. Major embarrassment leading to significant impact on effectiveness. Unacceptable operational impact, short term business interruption. Leads to material weakness.				
Moderate	Significant financial loss and variance to budget. Moderate embarrassment impacting short term effectiveness. Moderate operational impact, business not interrupted.Leads to reportable findngs.				
Minor	Minor financial loss, small budget variance. Minor embarrassment, but no harm to image or reputation. Minor operational impact, business not interrupted. Leads to audit findings.				
Insigificant or Neutral	Minimal or no measurable operational impact. Can be managed with routine activities. Leads to immaterial audit findings.				
	How to use this Tool: Assess your risk for levels of impact and likelihood. Find where the two values intersect. Use this intersection value to sort your risks and help with risk prioritization. Use your prioritization to help decide which risks require response strategies.				

Source: *ERM Playbook*

based on how the economy affects service recipients. Development of a forward-looking indicator can help an agency forecast risks likely to grow or decline in incidence or severity, so managers can take appropriate actions before risk materializes.

A risk indicator must be tested regularly to determine whether it reflects the actual risk taken. Sometimes a risk, such as a cyber-risk, may evolve in nature, and risk indicators should be refreshed to take account of those developments.

When key risk indicators have been developed, they can be illustrated in a dashboard format. Decision makers may benefit from being able to quickly review the range of major risks and their seriousness, compared with risk limits or other measures.

Heat Map

The heat map (see **Figure 2**) is a multi-colored, two-axis graph that charts the likelihood and impact of a range of risks. Colors on the graph range from green (for low-probability and low-impact risks) to yellow to red (for risks that have a high probability and high impact). A heat map allows the CRO to illustrate which risks are most important (i.e. those in the "red" zone vs. less important ones, in the "green" zone).

There are other ways to present the attributes of a range of risks. One of the most useful is a list of major risks, with vertical columns indicating attributes, and a series of red, yellow, or green indicators to show how the risk compares with others in terms such as likelihood, impact, risk velocity (i.e., how much time there is to respond), and whether the risk falls within or outside of the statement of risk appetite.

Risk Appetite Statement

The risk appetite statement specifies the amount of risk the agency is willing to take to achieve its objectives. Some agencies express risk appetite in terms of a four- or five-point scale. The Transportation Security Administration (TSA) is relatively far along in implementing ERM. The TSA Risk Appetite Statement from its ERM policy manual shows a scale ranging from "strongly averse," to "averse" to "risk neutral" and finally "risk tolerant." The TSA risk appetite statement is presented in **Appendix B**.[15]

Besides making an overall statement of risk appetite, agencies also should break down types of risk and make risk appetite statements about each. For instance, an agency may have virtually no appetite for taking risk on matters such as integrity and ethics, but may have a much greater appetite for risk in carrying out aspects of its mission. The office of comptroller of the currency, an agency with a mission quite different from TSA, also has a risk appetite statement that other agencies can use as a template.[16]

Risk appetite relates to the risk capacity of the agency (i.e., the amount of risk the agency can bear). Determining risk capacity requires an agency to consider the strength of its staffing, processes and systems, and the amount of risk these can take without serious damage occurring. A particularly difficult aspect of risk capacity relates to reputational risk and the danger that a relatively small event can cascade into a much more substantial reputational cost to the agency. On the other hand, a statement of risk appetite can help overcome the tendency of some agencies, and some civil servants, to shy away from taking risk as a way of avoiding adverse consequences, even at the cost of failing to achieve reasonable objectives. As with ERM, generally, the risk appetite statement seeks to help decision makers achieve a better balance and make reasonable risk-reward tradeoffs.

As with ERM, generally, the risk appetite statement seeks to help decision makers achieve a better balance and make reasonable risk-reward tradeoffs.

Risk Profile

Circular A-123 reflects a strategy of encouraging agencies to adopt ERM without specifically mandating it. This is an exceptionally wise strategy; if ERM were mandated it could become a compliance exercise rather than the flexible value-added tool it can be in the hands of an agency that wants to implement ERM.

Circular A-123 does impose one specific requirement: agencies must develop and maintain a risk profile, which "is a prioritized inventory of the most significant risks

identified and assessed through the risk assessment process…"[17] While agencies have discretion in shaping the content and format of their risk profiles, the circular specifies that a risk profile should include the following elements:

a. identification of objectives;
b. identification of risk;
c. inherent risk assessment;
d. current risk response;
e. residual risk assessment;
f. proposed risk response; and
g. proposed action category.

The circular categorizes objectives and requires the risk profile include strategic, operational, reporting and compliance objectives, and includes a helpful example of a risk profile (see **Appendix C**). Federal agencies are required to submit their risk profiles to OMB by early June each year.

Obtaining Feedback about Tools

As ERM evolves at an agency, experience will show which tools provide top management the greatest value for decision-making. The CRO office may use some tools to provide useful information for agency managers while using other tools during the internal analytical process. As always, a tool is only as good as the value it adds — in this case, to how an agency does business. User feedback can help decide which are the most appropriate tools to address an agency's risks.

> While some saw ERM as a "value add" in improving agency decision-making, others saw ERM as organizational self-defense.
>
> ›››

Building ERM into the Agency's Culture

It is remarkable how ERM has spread, thanks to a growing group of federal executives and managers who have seen its need and value, and — years before OMB issued guidance on ERM — created a movement to bring ERM to federal agencies. This movement was the origin of the Association for Federal Enterprise Risk Management (AFERM). The movement grew as the federal government saw a parade of scandals erupt at organizations, whose leaders were caught unaware and forced to resign. Often the repercussions included reputational damage as well as attacks on appropriations or civil service protections that affect the entire organization and not merely the place in which the risks originated. Thus, while some saw ERM as a "value add" in improving agency decision-making, others saw ERM as organizational self-defense. ERM is a recognized approach to surface major risks and deal with them before harm occurs. This stark history makes it easier to convince people up and down the hierarchy of the need for change, compared to other types of organizational change that may be more difficult to explain.

Building ERM into the agency culture involves creating a safe context in which managers and employees, up and down the hierarchy and across the organization, can share their concerns about major risks. Over time, as ERM yields increasing improvement in agency performance and decision-making, the cultural basis for ERM can continue to grow.

Embedding ERM into the agency culture can take years. At the Census Bureau, for example, which is an agency with some experience in implementing ERM, the chief operating officer sees ERM as a five-year process. As with any change effort, it's best to start with managers and parts of the organization most favorably disposed to ERM. Then, as other managers and units see how identification of major risks leads to a problem-solving response and an allocation of resources rather than a casting of blame, they can feel able to report major risks. As always, the tone at the top of the agency is critical to progress: a consistent message that blame attaches when an unreported major risk blows up — but usually not when the risk is reported in time to be addressed — can move the agency toward a culture that includes ERM.

ERM is a state of mind backed by a disciplined process. As the agency identifies, assesses, prioritizes and addresses major risks, the process begins to generate conspicuous success; then interviews and workshops and the various other ERM tools can yield increasingly greater value. The risk perspective is a way to increase, rather than limit, agency performance. To adapt the metaphor about cars going faster because they have brakes, the agency can gain a broad-based understanding that the car also can go faster if big potholes have been identified before there is a danger of hitting them.

> ERM can provide the greatest benefits when it is a part of the agenda of agency leaders, rather than simply an unsupported effort by the CRO.
>
> ‹‹‹

Special Issues: Leadership Transition, External Constraints and Political Decisions

Rotating Leadership: The U.S. political system generates rotating leadership every few years at almost all agencies. With the arrival of a new leader, who may be unfamiliar with ERM or preoccupied with some proposed major new initiative, the CRO and agency career managers will need to persuade the new leader to allow ERM to proceed at the agency. The best approach is to allow the incoming head to hear about ERM from a variety of sources. A review of Circular A-123 can aid in explaining the importance of ERM to the new leader.

The CFO may be another major player, especially given the broad support federal

CFOs have shown for ERM. The outgoing agency leadership may point to ERM as a valuable tool for their successors. It is during a transition that an agency culture favorable to ERM shows its value. The incoming political leadership may be impressed if agency senior executives state that ERM is the way the agency *does* business, while OMB simultaneously indicates ERM is the way the agency *should do* business. The CRO should avoid making enemies, for instance by pushing too hard when there is no political official in place to provide the needed support and tone at the top. ERM can provide the greatest benefits when it is a part of the agenda of agency leaders, rather than simply an unsupported effort by the CRO.

The CRO may be able to show incoming leaders the value of ERM by preparing an introductory major risk report about the agency. New leaders want to move quickly to establish their agendas. They understand the need to learn quickly about any major problems inherited from their predecessors. The report can help the incoming leadership by showing that a risk function already in place has scanned the horizon for major risks the agency needs to address.

External Constituencies: Another important aspect of the U.S. political system is the extent to which external constituencies — and especially those in the legislative branch of government — can induce an agency to take on more (or greater) risks than leaders might prefer, or preclude the agency from taking action to avoid, transfer or mitigate risks in ways the ERM process suggests. In these cases, ERM can help agency leadership find the most acceptable ways of dealing with the risk, and can generate data-based information to show external constituencies the risk consequences of specific courses of action, along with alternatives.

Budgeted Resources: The congressional appropriations process may involve uncertainty as well as temporary or long-term resource limitations imposed on an agency. In Fiscal Year 2013, before ERM was prevalent in the federal government, many agencies suffered from a sequestration of funds that caused substantial and unexpected agency budget cuts. Had an ERM process been in place, the CRO could have generated alternative ways of dealing with the cuts and the risks each alternative involved. Agencies that sought to avoid furloughs or layoffs by offering buyouts to staff, for example, may have lost key people with skill sets hard to replace. A strong ERM process could have anticipated that risk and suggested alternative human resources approaches.

Moreover, in the current uncertain budget environment a robust ERM process can suggest ways to manage against potentially serious budget constraints, for instance by implementing succession planning so key managers and employees have trained successors should they decide to leave. In other words, because of the forward-looking analyses it generates, ERM is an excellent way to more effectively manage a range of externally imposed constraints and the associated major risks.

Political Leadership: An agency's political leadership, even when faced with a credible statement of major risks, may still decide on a risky course of action. This is beyond the scope of ERM. The function of ERM is to provide decision makers the best available information about major risks so they can make the best risk-reward tradeoffs. Once informed, a senior leader has the power and authority to make any decision. ERM is a management tool to help advise decision-makers, but the final decision is theirs to make.

Had an ERM process been in place, the CRO could have generated alternative ways of dealing with the cuts and the risks each alternative involved.

Indicators Whether ERM Is Working

The CRO will know ERM is working when managers and employees at all levels of the organization feel free to report risk-related issues up the line, and when top management supports a robust risk-prioritization process and the allocation of resources to deal with the highest priority risks. One survey that provides a rough indicator for the federal government, albeit with a significant lag time, is the Federal Employee Viewpoint Survey (FEVS). In general, only three-fifths of respondents across the federal government report "I can disclose a suspected violation of any law, rule or regulation without fear of reprisal."[18] The U.S. Office of Personnel Management makes subsets of the survey available to individual agencies to learn the views of their own employees. Because the FEVS obtains only general information, and with a lag time, the risk office may want to conduct its own smaller surveys, targeted at perceptions of the risk function. Similar issues likely exist for employee surveys conducted at state and local levels of government.

A critical question for the CRO is whether ERM is a working reality at the agency, or merely a gesture that adds little or no value to agency decision-making. Clifford Rossi, an experienced risk manager who teaches at the University of Maryland, looked at financial institutions in the financial crisis and found what he called "symptoms of risk dysfunction." While those symptoms are derived from private-sector experience, the implications for government are apparent:

1. low morale and self-esteem among risk managers;
2. openly derisive comments and attitudes toward risk staff;
3. high turnover in risk functions: voluntary and involuntary;
4. increasingly combative and aggressive posture toward risk management;
5. lack of stature of risk management; and
6. risk management viewed as a cost center.[19]

While these indicators are suggestive, the position of risk managers in a government agency can be seen in one key indicator: the risk function is not working when people simply fail to provide information to the CRO except on the most superficial level. In the government agency context, holding back information is, perhaps, the most aggressive posture a manager or employee can take. ERM is not working when it turns into a series of meetings and reports rather than a useful risk-management tool.

If the CRO feels the process is slipping, the first task is to gain more information from trusted colleagues about why the risk function is not seen as a source of value for the agency. As is often the case, good preparation may be key: if the CRO has built a constituency across the agency, it will be much easier to obtain solid information about steps to improve the status of the risk function. Next, gauge the posture of top management to ERM. Sometimes, specific problems can be addressed directly. For instance, the CRO can determine a product of demonstrable value that the risk function can offer top management. Consulting with trusted colleagues at other agencies, can provide useful ideas. Not all problems — especially a lack of tone at the top — can be resolved, but making the effort is worthwhile. If nothing seems to work, it may be time to focus on bringing ERM to large subordinate units of the agency where the leaders understand the value, and welcome the improved management strength that comes from ERM.

Making Progress: Indicators of ERM Maturity at an Agency

Two tools can help assess the state of ERM at an agency. The risk management assessment framework, developed in the United Kingdom (UK) by their equivalent of OMB, can help determine the state of ERM in an agency.[20] The framework builds on questions, slightly adapted and expanded here so they explicitly focus on ERM:

Capabilities

1. Leadership: do senior management and department heads support and promote ERM?
2. Are people equipped and supported to identify and manage major risks well?
3. Does the agency prioritize risks well and allocate resources appropriately to deal with them?
4. Is there a clear ERM strategy, and ERM plans and policies?
5. Are there effective arrangements for managing major risks with partners?
6. Do the organization's processes incorporate effective ERM?

Addressing Risks and Achieving Outcomes

7. Are major risks well addressed?
8. Does ERM contribute to achieving outcomes?

The risk assessment framework provides a five-point scale to assess the state of risk management now and at regular intervals. The UK document, *Risk Management Assessment Framework: A Tool for Departments*, should be reviewed, adapted to an agency's circumstances and to ERM specifically, and applied as a self-diagnostic tool.

The second valuable tool is the U.S.-based risk maturity model, which agencies use to assess progress from a nascent ERM program to one more robust, and built into agency processes and the culture. The *ERM Playbook* contains examples of several maturity models agencies may wish to adapt.

The CRO can share one of these templates with the risk management committee each quarter or half-year, along with an assessment of where the agency falls along the maturity model. Discussion of where the agency falls on the risk assessment or maturity scale, and what might be done to advance the agency, can prove fruitful. The progress report also can be shared more widely within the agency, to obtain feedback and suggestions about how to make further progress. ◁

Conclusion: ERM for Strengthening Agency Management, Culture and Performance

In summary, ERM is a tool that can help protect agencies and their leaders, managers and employees, from the harm of an unexpected major risk that materializes. By preparing ahead, an agency can reduce the probable impact of a major risk and, perhaps, the odds of negatively impacting agency resources (e.g. funding or human resources), mission delivery and reputation, or causing any harm at all. ERM is also a tool to inform and improve agency decision-making and performance; but that presents a case less apparent to agency leaders who believe themselves already capable of making good decisions.

ERM does not require a new bureaucracy or management layer. Rather, ERM requires that the agency change the way it does business, to free the flow of risk information — up and down the hierarchy and across organizational silos. The CRO is a facilitator rather than a compliance officer, and can be extremely valuable to the organization. The CRO's major task is to elicit important risk information. The CRO's role is also analytical — to distinguish valid warning signs, to search for root causes, and to support a risk management committee that, as a body, serves as an advisor to review risks, prioritize them and present them to the agency head or COO.

This type of facilitative and advisory process can be foreign to many agencies. That's why "quick wins" may be needed to assure leaders, managers and employees not only of the value of ERM but also that the process seeks to generate insights and information, rather than directives others must follow. Risks become a part of normal operations, to be dealt with in a business-like way without assigning blame. The mantra of top management should become: "I want to hear about major risks from you before, rather than after, they appear in an inspector general report or the newspaper." This should be an appealing approach for agency leadership, political and career, especially in the context of growing complexity of programs and operations, and the growing probability that complexity itself can engender major risks that require cross-agency attention to detect.

As growing numbers of government agencies turn to ERM, collaboration may be the best approach. By learning from colleagues at other agencies and different levels of government, and sharing experiences, risk officers can strengthen one another and, by extension, operations across the government.

Appendix A: Recommended Reading

Government Documents

Office of Management and Budget, OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, July 15, 2016.

Office of Management and Budget, OMB Circular No. A-11, *Preparation, Submission, and Execution of The Budget*, Section 270, "Performance and Strategic Reviews; Enterprise Risk Management," pp. 270-13 to 270-16.

Chief Financial Officers Council and Performance Improvement Council, *Playbook: Enterprise Risk Management for the US Federal Government*, July 29, 2016., refered to as *ERM Playbook*.

HM Treasury (UK), *Risk Management Assessment Framework: A Tool for Departments*, July 2009.

US Government Accountability Office, *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risks*, GAO-17-63, forthcoming.

Books and Other Materials

John Fraser and Betty J. Simkins, *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*, Hoboken, NJ: John Wiley & Sons, Inc., 2010.

Anette Mikes, "Enterprise Risk Management at Hydro One (Multimedia)," Boston, MA: Harvard Business School, June 2010.

Anette Mikes, "The Triumph of the Humble Chief Risk Officer," Harvard Business School, Working Paper 14-114, May 23, 2014.

Thomas H. Stanton and Douglas W. Webster, eds., *Managing Risk and Performance: A Guide for Government Decision Makers*, Hoboken, NJ: John Wiley & Sons, Inc., 2014.

Douglas W. Webster and Thomas H. Stanton, *Improving Government Decision Making through Enterprise Risk Management, IBM Center for the Business of Government*, 2015, available at www.businessofgovernment.org.

Publications of Standards Organizations

Committee of Sponsoring Organizations (COSO), *Enterprise Risk Management: Aligning Risk with Strategy and Performance*, Public Exposure Draft, June 2016 edition.

Dr. Patchin Curtis and Mark Carey, Deloitte & Touche, LLP, "Risk Assessment in Practice," COSO, October 2012

International Standards Organization, *ISO 31000:2009 — Risk management — Principles and guidelines*, 2009.

Appendix B: Risk Appetite Statement from the Transportation Security Administration (TSA)

Transportation Security Administration

Appendix 4: TSA Risk Appetite Statement

The TSA ERM policy specifies ERM practices and applies to all TSA Program Offices at headquarters, in the field, and to employees at every level of the organization. This appendix consists of the appetite statements presented in that policy.

TSA creates value by protecting the Nation's transportation systems while enabling the movement of legitimate travelers and goods. TSA seeks practical and cost-effective solutions to effectively reduce the most significant transportation security risks.

TSA has different appetites for different risk types expressed in the following statements:

- TSA is strongly averse to security risks that could result in catastrophic consequences.
- TSA is strongly averse to the compromise of classified information and averse with regard to the compromise of Sensitive Security Information (SSI) and Personally Identifiable Information (PII).
- TSA is averse to workforce-related risks pertaining to integrity, performance, health and safety, and regulatory compliance.
- TSA is averse to events that could damage its standing and reputation with the traveling public, U.S. Congress, and other federal and industry stakeholders.
- TSA is risk neutral with regard to other mission and business operational enterprise risks.
- TSA is risk tolerant to programs that enhance the movement of legitimate travelers and goods.

TSA makes risk-informed decisions to achieve its mission within the parameters of its risk appetite:

- TSA evaluates and manages risks to the five transportation modes for which it is responsible arising from international terrorists, homegrown violent extremists, insiders, or other adversaries.
- TSA considers the interconnected and interdependent nature of the physical, human, and cyber components of the transportation infrastructure when assessing risks and response plans.
- TSA recognizes the need to balance security effectiveness with operational efficiency, cost, industry vitality, and passenger satisfaction by taking a systems approach to risk management.
- TSA evaluates the highest risk scenarios and the effectiveness of layered security counter-measures using advanced computational techniques to apply finite resources commensurate with the risk level.

Appendix C: Sample Risk Profile from OMB Circular A-123

STRATEGIC OBJECTIVE – Improve Program Outcomes								
	Inherent Assessment		Current Risk Response	Residual Assessment		Proposed Risk Response	Owner	Proposed Risk Response Category
Risk	Impact	Likelihood		Impact	Likelihood			
Agency X may fail to achieve program targets due to lack of capacity at program partners.	High	High	REDUCTION: Agency X has developed a program to provide program partners technical assistance	High	Medium	Agency X will monitor capacity of program partners through quarterly reporting from partners	Primary – Program Office	Primary – Strategic Review
OPERATIONS OBJECTIVE – Manage This Risk of Fraud in Federal Operations								
Contract and Grant fraud.	High	Medium	REDUCTION: Agency X has developed procedures to ensure contract performance is monitored and that proper checks and balances are in place.	High	Medium	Agency X will provide training on fraud awareness, identification, prevention, and reporting.	Primary – Contracting or Grants Officer	Primary – Internal Control Assessment
REPORTING OBJECTIVE – Provide Reliable External Financial Reporting								
	Inherent Assessment		Risk Response	Residual Assessment		Proposed Action	Owner	Proposed Action Category
RISK	Impact	Likelihood		Impact	Likelihood			
Agency X identified material weaknesses in internal control.	High	High	REDUCTION: Agency X has developed corrective actions to provide program partners technical assistance.	High	Medium	Agency X will monitor corrective actions in consultation with OMB to maintain audit opinion.	Primary – Chief Financial Officer	Primary – Internal Control Assessment
COMPLIANCE OBJECTIVE – Comply with the Improper Payments Legislation								
Program X is highly susceptible to significant improper payments.	High	High	REDUCTION: Agency X has developed corrective actions to ensure improper payment rates are monitored and reduced.	High	Medium	Agency X will develop budget proposals to strengthen program integrity.	Primary – Program Office	Primary – Internal Control Assessment and Strategic Review

Endnotes

1. OMB Circular A-123 similarly defines ERM as "an effective Agency-wide approach to addressing the full spectrum of the organization's external and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos. ERM provides an enterprise-wide, strategically-aligned portfolio view of organizational challenges that provides better insight about how to most effectively prioritize resource allocations to ensure successful mission delivery."
2. Sydney Finkelstein, Jo Whitehead, and Andrew Campbell, *Think Again: Why Good Leaders Make Bad Decisions and How to Keep it From Happening to You* (Harvard Business Press, 2008)
3. This guide refrains from entering into questions such as whether the term "risk" should be defined as including uncertainties that reflect positive as well as negative developments. In the end, ERM needs to address both risks of harm occurring and risks of missing opportunities. Those with an appetite for such questions will need to consult leading frameworks such as ISO 31000:2009, "Risk management – Principles and guidelines," and the COSO standard, currently under development, "Enterprise Risk Management: Aligning Risk with Strategy and Performance."
4. Thomas H. Stanton, *Why Some Firms Thrive While Others Fail: Governance and Management Lessons from the Crisis* (Oxford University Press, 2012).
5. Ibid.
6. The concept of constructive challenge has been explored most intensively with respect to the role of boards of directors vis-à-vis their CEOs. Jeffrey A. Sonnenfeld, "What Makes Great Boards Great," Harvard Business Review, September 2002, pp. 106-113, explores cultural tone and preconditions of constructive challenge that are directly relevant to the government context as well. The concept of constructive dialogue is set forth in Thomas H. Stanton, "Constructive Dialogue and ERM: Lessons from the Financial Crisis," chapter 32 of John R. Fraser, Betty J. Simkins, and Kristina Narvaez, I*mplementing Enterprise Risk Management: Case Studies and Best Practices*, 2014.
7. Anette Mikes and Robert S. Kaplan, "Towards a Contingency Theory of Enterprise Risk Management," Harvard Business School, Working Paper 13-063, Jan. 13, 2014. ("Our conclusion is that effective risk management 'depends'; it is contingent on the organization's context and circumstances.")
8. Institute of Internal Auditors, "IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control," January 2013. The third line of defense would include the agency inspector general or the internal audit function, for example.
9. Anette Mikes, "The Triumph of the Humble Chief Risk Officer," Harvard Business School, Working Paper 14-114, May 23, 2014.
10. Nancy Potok, Deputy Director and Chief Operating Officer, US Census Bureau, "US Census Bureau: Operationalizing ERM – A Top-Down, Bottom Up Approach," AGA DC Chapter Training, March 2016, slide 10. The wording of the seven steps has been edited slightly.
11. See, e.g., Thomas H. Stanton, "Risk Management and the Dynamics of Budget Cuts," chapter 10 of Thomas H. Stanton and Douglas W. Webster, eds., *Managing Risk and Uncertainty: A Guide for Government Decision Makers* (John Wiley & Sons, Inc., 2014); and, for an excellent analysis of risk-based budgeting in the private sector context, "Cut Costs to Grow Stronger," chapter 5 of Paul Leinwand and Cesare Mainardi, *Strategy That Works: How Winning Companies Close the Strategy-Execution Gap* (Harvard Business Review Press, 2016).
12. Federal Student Aid Annual Report FY 2016, pp. 49-50.
13. Mikes and Kaplan, supra note 7, p.29.
14. For an excellent example of application of voting techniques in a workshop, see *Enterprise Risk Management at Hydro One (Multimedia),* Boston, MA: Harvard Business School, June 2010.
15. Transportation Security Administration, Enterprise Risk Management, ERM Policy Manual, "Appendix 4: TSA Risk Appetite Statement," pp. 56-57, August 2014, available at www.aferm.org/resource/tsa-erm-policy-manual/, accessed September 2016.
16. The OCC risk appetite statement can be found at www.occ.treas.gov/news-issuances/news-releases/2016/nr-occ-2016-44.html, accessed September 2016.
17. OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, July 15, 2016, p. 13.
18. Office of Personnel Management, *2015 Federal Employee Viewpoint Survey Results*, p. 28.
19. Clifford Rossi, "Removing Barriers to Pathological Risk Behavior: The Art of Effective Communication," presentation at the AFERM Summit, Sept. 18, 2012.
20. HM Treasury, *Risk Management Assessment Framework: A Tool for Departments*, July 2009. While the UK has not adopted ERM explicitly, HM Treasury documents are based on a concept of integrated risk management that is quite comparable.

www.agacgfm.org