*EARLY DRAFT*

*Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*, second edition, John R.S. Fraser (Editor), Rob Quail (Editor), and Betty Simkins (Editor), 2021

**Chapter 12: Increasing Adoption of Enterprise Risk Management in the US Federal Government**

Thomas H. Stanton **1**

Former President of the Association for Federal Enterprise Risk Management (AFERM)

By a process of trial, error, and success, practitioners of Enterprise Risk Management (ERM) in the US government have come to recognize the importance of cultural change as necessary to achieve buy-in from the political leadership, career senior executives, and staff of government departments and agencies.2 Because ERM depends on eliciting information from across an enterprise and up-and-down the hierarchy, cultural acceptance is needed to make ERM a practical reality. The way that ERM has spread in the federal government reflects the unusual institutional characteristics of the US government compared to characteristics of more centralized administrative states such as exist in the United Kingdom, Canada, and Australia, which are three other countries that have sought to make ERM a feature of public management.

This chapter begins by recounting the origins of ERM in the US federal government in the early 2000s. ERM practitioners adopted a network model of bringing ERM to management practices in an increasing number of agencies. A network approach was effective, not only because of the decentralized nature of the US federal government, but also because, as the second section explains, ERM itself is more robust when managers practice it as a way of increasing the performance of their organizations rather than merely because a central body tells them to adopt ERM. The second section carries this theme forward with a series of examples about why agencies adopt ERM, how adoption is best implemented as a process of cultural change, and how ERM becomes institutionalized and embedded in agency processes. The third section contrasts the implementation of ERM in a private company with ERM in a government organization that is susceptible to a range of political forces and consequent major nonquantifiable risks, including oversight from a US Congress that is not always seeking to enhance managerial effectiveness of an agency. The fourth section seeks to parse the unusual administrative structure of the US government compared with more centralized parliamentary systems. The chapter concludes with a brief examination of useful next steps for the continuing spread and institutionalizing of ERM in US government agencies.

**Origins of ERM in the US Federal Government**

Led by Douglas W. Webster, Chief Financial Officer of the US Department of Labor, eight current and former senior federal officials, mostly from the community of Chief Financial Officers, met in 2008 to collaborate on developing a risk-based approach to agency decision-making in their respective departments and agencies.3  Sallyanne Harper, then Chief Financial Officer at the Environmental Protection Agency (EPA) and one of the seven founders of the ERM movement in the federal government, explains the motivation for the meeting:

“A number of us had experience in agencies that routinely managed risk at a programmatic level (for instance, at EPA virtually every program had developed a sophisticated risk assessment and risk management approach…). What we did not have was a risk profile and risk assessment that crossed programmatic lines, took into account shared risk potential or considered the agency-wide portfolio view. Therefore we lacked a consistent approach to resource allocation decisions or other agency-wide strategic and tactical decisions that consistently understood and took portfolio risk into account. We also did not have a consistent lexicon to use to discuss risk across programs and at the agency level. That was very frustrating when we clearly could see how important it was to be able to improve decision-making.” (Sallyanne Harper, personal communication, January, 2020)

The group decided to hold a conference that year on Enterprise risk management to try to attract like-minded officials and consultants from across the federal government. With support from the business school of George Mason University, the annual event gained in popularity. Sustained interest in federal ERM grew each year. The small original group of federal executives then formally established the Association for Federal Enterprise risk management (AFERM), with Dr. Webster as the founding President. At this writing, a dozen years later, AFERM has become a community of practice of some 600 members that holds an annual conference attracting hundreds of people each year. AFERM maintains a robust website ([www.AFERM.org](http://www.AFERM.org)) and holds quarterly lunches and other events to share ERM insights from leading agencies. Federal ERM practitioners have published several books on ERM (Stanton and Webster, 2014; Hardy, 2015; Fletcher and Stanton, 2019) that have gained widespread readership in the federal ERM community. Exhibit 1, below, presents AFERM’s 2020 strategic plan as the organization continues to build its presence.



**Exhibit 1: AFERM Strategic Plan**

Despite initial disinterest from the Office of Management and Budget (OMB) and the Government Accountability Office (GAO), AFERM continued to reach out to try to show the value of ERM as a federal management tool. In 2013, AFERM invited John Fraser, leading Canadian ERM practitioner and author (See, e.g., Harvard Business School/Mikes, 2010), to meet informally with officials at OMB. As the federal ERM movement grew, OMB officials became strong supporters of ERM and in 2016 issued guidance (OMB, 2016) calling on federal agencies to submit annual “risk profiles” listing major risks and how the organization is addressing them.

In addition, the Chief Financial Officers Council and Performance Improvement Council, two network organizations operating under OMB’s auspices, published a *Playbook: Enterprise risk management for the US Federal Government* (2016) to help guide agencies through the practical and technical aspects of establishing ERM at an agency. At this writing in 2020, perhaps 20-25 percent of federal agencies practice serious ERM (a rough estimate), and the numbers continue to grow. The combination of firm guidance from the management side of OMB, and support from a coalition of risk managers at federal departments and agencies has proved to be a winning one, leading – among other consequences – to a substantial increase in membership in the Association for Federal Enterprise risk management.

**Implementing ERM at a Federal Agency: The Importance of Cultural Acceptance**

1. Why Government Agencies Adopt ERM

Federal agencies adopt ERM for a variety of reasons. Often a new agency head will request the establishment of ERM because it is already familiar to him or her as a powerful management tool. Thus an incoming senior military official led the Defense Logistics Agency to establish an exemplary ERM function (Stagnitti, 2014). After the Financial Crisis, the incoming Treasury Assistant Secretary for Financial Stability arrived from a position at Goldman Sachs, a firm that possessed a strong risk management function, and called for the establishment of ERM processes to help safeguard the financial integrity of the Recovery Act that dispensed hundreds of billions of dollars in an effort to promote economic recovery after the Crisis.

Some incoming agency heads learn from others. Lisa Mensah, a new Undersecretary of Agriculture for Rural Development saw how the Treasury Department was establishing ERM and sought guidance on how to do the same in her mission area. At the US Department of Commerce, an Undersecretary who arrived from a position in the private sector used his position to promote ERM at the agencies in the Department of Commerce. The process gained strength when Dr. Nancy Potok, his Deputy Undersecretary, became Chief Operating Officer of the US Census Department and began a five-year program of ERM implementation. As Dr. Potok explained in a 2014 interview, she saw ERM as essential for managing her agency well:

“From my vantage point as COO of a billion dollar organization with 17,000 employees who are involved in diverse activities across the country, it is impossible to know the important risks to our mission simply by relying on people deciding to tell me. In government in particular, it’s very difficult for people to bring you bad news. They don’t want to tell you when things are going wrong for fear of being blamed and punished. They try to fix things themselves, even when they need help. As a consequence, the higher up you get in the organization, the later you find out about the serious challenges.

Of course, the later you find out about challenges, the harder they are to address. What I wanted to create is a climate where people feel comfortable coming forward with things they need help with at a stage when it’s still relatively easy to help them, as opposed to dealing with a full blown crisis much later down the line.”

Yet other agencies come to ERM after suffering substantial harm when a serious risk materializes. A major case involved the Internal Revenue Service (IRS), which suffered major reputational risk and consequent substantial congressional cuts in its budget. This happened when managers of the IRS process for approving applications for tax exemptions to social welfare organizations, applied an impolitic criterion to screen applicants that aroused significant congressional ire (e.g., Rappeport, 2017).

Finally, some agencies adopt ERM after experiencing the value of applying a risk-based approach to their mission. Some years ago, the Transportation Security Administration (TSA) instituted a risk-based program that created substantial value, for airlines, the traveling public, and for TSA itself. TSA has a dual mandate: to ensure that the wrong people don’t get onto airplanes and to help travelers go through screening without undue delays. The latter mandate relates to potential repercussions: intolerable delays and angry complaints from the flying public would likely precipitate a congressional reaction that, if inartfully designed, could reduce the ability of TSA to protect airline security.

TSA’s risk-based solution was to segment the queue of passengers waiting to get onto aircraft, into riskier and less risky segments. The agency developed the system known in the United States as PreCheck. Travelers may apply for PreCheck status by providing significant background information that TSA then verifies against commercially available databases. Travelers who pass the background check can take advantage of a reduced airport screening process. Other travelers, without PreCheck status, must undergo more thorough (and time-consuming) screening at the airport. To reduce chances of someone gaming the system, a certain percent of PreCheck travelers is assigned to undergo the more thorough screening process. Risk-based management yielded significant benefits, including substantial cost savings and reduced staffing requirements. (Stewart and Mueller, 2016). The success of the TSA’s PreCheck process led to an increased appreciation of the value of effective risk management and led to TSA becoming an early agency to adopt ERM.

1. Adopting ERM as a Process of Cultural Change

Experience has shown that ERM proceeds best at a government agency if it is addressed in a process of cultural change, rather than as a mere compliance activity. Telling people to practice ERM is not nearly as successful as selling them on its importance. Requiring an agency to report its five major risks, for instance, could prompt proforma compliance without actually undertaking a serious process of risk identification, assessment, and prioritization. A process of cultural adaptation, while more difficult than simply demanding compliance, can allow an agency to apply ERM as a systematic way to add value to the way that it does business.

The Rural Development mission area of the US Department of Agriculture (USDA-RD) provides an example of promoting cultural acceptance by bringing unit heads early into discussions about ERM and how it can benefit them and their organizations. The Undersecretary for Rural Development invited the present author to work with her senior staff to prepare to adopt ERM. She, her chief of staff, the Chief Financial Officer, and the present author met weekly as an ERM planning team to set a course for adopting ERM, measure progress and adapt according to feedback from the organization. The process included multiple steps over several months:

1. The Undersecretary convened a meeting of senior staff, including both political and career executives, to discuss ERM and why other agencies were adopting ERM as a management approach.
2. She then asked the present author to interview senior staff individually to discuss ERM, answer their questions and address their concerns, and to gain a preliminary understanding of the major risks that they saw facing USDA-RD. These individual conversations allowed senior executives to help shape ERM as it was rolled out, and also achieved buy-in. For instance, senior executives expressed concern about draining scarce executive and staff resources to build a large ERM unit. As a result, the Undersecretary and her team could address that concern by proposing only a small ERM office.
3. The ERM planning team hosted a series of brown-bag lunches at which Chief Risk Officers (CROs) of other government agencies presented their experiences and showed how ERM added value to their agencies. The brown-bag lunch helped to foster an atmosphere of informality so that curious executives could ask questions and learn how ERM worked in practice. The Undersecretary broke from her busy schedule to attend some lunches, thereby increasing the attraction of the lunches as good for an official to attend.
4. As a part of the process of cultural change, USDA-RD invited the present author to travel to a meeting of field staff to address several hundred officials about ERM and what the central office was thinking about.
5. The ERM planning team then prepared a position description for the new Chief Risk Officer. The planning team also prepared a governance document for a new Risk Management Committee that would help the Undersecretary to understand the portfolio of major USDA-RD risks and prioritize them. Both documents built on comparable documents from other agencies and some examples that the 2016 *Playbook* presented. The planning team considered the two documents in several iterations as it deliberated how best to craft them to meet the needs of USDA-RD.
6. USDA-RD then posted a job announcement to hire a Chief Risk Officer at the senior executive level, and hired a new CRO. It turned out that the new CRO was a senior executive with a strong record in other parts of USDA-RD. That was a wise decision since it tends to be easier to teach ERM to a seasoned and respected executive than to teach an ERM expert about the particular organizational culture of an agency with which they are unfamiliar.
7. The Undersecretary then selected members of the Risk Management Committee. These were people from diverse parts of USDA-RD. They were largely senior executives who had shown sensitivity to the welfare of the overall organization rather than focusing narrowly on the particular units they headed.
8. The new CRO, supported by members of the ERM planning team, briefed other parts of the Department of Agriculture, including the departmental Inspector General, the departmental Office of Budget and Program Analysis, and later (after the Undersecretary departed as part of a change of presidential Administration) the transition team of the incoming Administration.
9. Responding to concerns about staff limitations that executives had raised, USDA-RD allocated funds for two years of consultant support for the new small CRO office. The contract specified that the consultant would strengthen the capabilities of the CRO rather than assuming functions for itself.
10. The office continues to show value as it plays its role. Other parts of the Department of Agriculture have now expressed interest in adopting ERM for themselves.

Proponents of ERM, wherever located in the organization, often are able to build constituencies for ERM and bring people to the table to share information about major risks. Some agencies build risk-awareness into the performance goals of their senior executives. At one agency, the Chief Financial Officer has set three categories of funding for the next fiscal year: (1) core mission functions, (2) new mission functions, and (3) to address major risks. This approach echoes approaches of other CFOs who have encouraged reluctant unit heads to share their information about risks as a way to obtain needed resources.

Kenneth Fletcher, TSA’s first Chief Risk Officer, notes that a process of culture change management was needed to help TSA to develop both PreCheck and the more comprehensive ERM program. As Fletcher (2019, p. 19) has recounted, the process of cultural change was multifaceted:

* “Leveraging existing passenger information known by the US Government and the airlines;
* Broad-based internal engagement during development;
* Extensive engagement with airlines and airports;
* Frequent status briefings with Department of Homeland Security leadership, the National Security Council, and congressional oversight committee staff;
* Regular communications with the entire TSA workforce celebrating wins and improving status;
* Field visits and townhall sessions by the Administrator, Deputy Administrator and Agency executive leadership;
* Creating and sustaining a sense of urgency and purposefulness with aggressive performance goals;
* Risk-Based Security performance goal added to all agency executive performance plans; and
* External engagement and validation with academia and the intelligence community”

Chief Risk Officers understand the need to turn ERM from a concept into an effective practice that adds value. They must be interpersonally sensitive and impose only minimal burdens on busy senior executives. A successful CRO can show value to those executives through “quick wins” that resolve major annoyances that might not involve major risks but that can show key leaders the value of the ERM function and its enterprise-wide knowledge of the agency and its processes. 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 a large number of these reports could be eliminated, thereby reducing burdens on management and making it more likely that information in the remaining reports will be read and used.

To take another example, Frank Vetrano, Chief Risk Officer of the Federal Housing Administration (FHA), found that a large number of the agency’s information technology contracts were due to expire within a single year and that the relevant contracting office lacked the capacity to renew many of those contracts. In past years, one result had been intense friction among agency units to push their contract renewals to the head of the queue. Other results were dysfunctional use of contracting work-arounds such as contract extensions even though the needed scope of work had changed, or shifting of the contract work to another vendor that possessed an open contract vehicle that would allow quick assumption of the work. Once the CRO office surfaced and analyzed the problem, it was possible to create a system of prioritization of the most important contracts for renewal and allocation of added resources to the contracting function.

Through such “quick wins” Mr. Vetrano used the CRO office essentially as a management consultant to the agency and thereby won the confidence of the people heading major units. As Mr. Vetrano explains, there are limits to this approach:

“…the consultative approach may not work in all cases, and a certain amount of tension between a centralized risk function and program areas is natural and healthy. For example, part of a risk management function’s responsibility is to ask tough questions when appropriate, which can cause discomfort and possibly reinforce misgivings that a program office might hold toward a risk oversight group. Our advice - It’s probably best not to start with those areas where there are likely going to be a number of problems that require attention and challenges that must be overcome. A risk office has considerable flexibility in prioritizing projects to tackle. If possible, start with a few significant problems that particularly concern individual program areas. The goal is for the risk function to earn respect and credibility early on so that the tough conversations can take place later.” (Vetrano and Stayanovich, 2019, p. 34).

Chief Risk Officers of other agencies have documented how a risk-based approach not only has helped to manage a major risk but also has facilitated improved management more generally. Such examples often relate to problems of long queues and the way that a large backlog of people or organizations seeking government services can be an indicator of a major risk that often may be addressed through a risk-based management approach.

The Internal Revenue Service (IRS) was an agency that came to ERM after an unexpected incident materialized that caused significant harm. The IRS is an example of the opposite sequence from TSA: IRS put ERM and a new Chief Risk Officer in place and this allowed the agency to develop a risk-based approach to a problem of an unacceptable backlog. As noted above, the Internal Revenue Service (IRS) suffered major reputational risk and consequent substantial congressional cuts in its budget. When the dust settled and the IRS was under new management operating with a much-constrained budget, the new Chief Risk Officer, David Fisher, learned through the newly established enterprise risk management processes that the IRS approach for reviewing applications for a similar kind of tax exemption – charities – also was faced with significant operational and reputational risks. That risk came from small organizations, established for instance by parents whose child had died from an incurable disease and who sought to raise money for the cause, whose applications languished many months at the IRS awaiting approval.

Working with others at the IRS, including officials in the relevant unit, Mr. Fisher realized that such applicants, with a very appealing claim to quick approval, could take their justifiable complaints about long waiting times to a Congress ready to pounce once again on the IRS. To address the situation, the team devised an alternative risk-based solution in which applications would be placed into two distinct tracks. In the “lower risk” track were applications from small groups who anticipated collecting donations only below a certain threshold amount. These applications would be given approval with a much lighter screening process. As a control, applicants would certify under penalty of perjury that the facts in their applications were correct and in compliance with all statutory requirements. The risk of a false application would be small because the amounts involved in fundraising would be small. Moreover, the IRS would have the opportunity to audit those organizations after they began operation. The IRS also could audit a small proportion of these applications to determine the incidence of tax avoidant behavior. The IRS created a simplified application form for users of the simplified process. The IRS then set aside in a second track the larger and more complex applications that did require up-front screening because of the potentially greater amounts of tax revenue involved in granting a tax exemption. The risk-based approach had an additional benefit: the IRS would save resources that it had devoted to screening small applications and could apply them to provide faster and better screening of the larger applications. (See, e.g., IRS, 2017). The throughput for both processes was dramatically improved, and published reports indicate a low incidence of fraudulent behavior by those entities going through the streamlined process.

Mr. Fisher, now a partner at a private sector consulting firm, stated (personal communication to the author, February 2020) that:

“We collectively realized that our risk appetite for this business process was out of sync, trying to force all these applications through a highly risk averse process. By using data to create a second path, a streamlined path, for lower risk transactions, the entire system improved. In addition to clearing out the entire backlog in less than 100 days, the throughput time for the lower risk charity applications became almost instantaneous while the higher risk applications were processed in about one-third of the original time. Moreover, audits showed that the incidence of fraud was almost non-existent.”

1. Implementing ERM at an Agency

Dr. Nancy Potok (2015), then Chief Operating Officer of the US Bureau of the Census, has suggested 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.”

Support from the top of the organization, and active engagement by the agency head or deputy, are essential for making ERM a success in an agency. Selling ERM as a management approach requires addressing needs and perspectives of political officials differently from those of senior executives and staff. For an incoming political head of an agency, ERM is a good way to survey the risk landscape to understand major risks, inadequately addressed by a predecessor, that have the potential to disrupt the new official’s tenure and reputation. Agencies are finding that ERM can be presented to incoming officials as “the way that we do business.” This can be a strong argument, especially when combined with OMB requirements that agencies submit risk profiles annually.

If top-level support and active engagement are not forthcoming, it is probably wise to move the ERM function to a lower level organization where leaders are more open to ERM. Top-level support is needed both to engage powerful unit heads in discussion of major risks and to elicit information about those risks so that they can be assessed, prioritized, and addressed appropriately. There tend to be disparities in the time it takes for different units in an organization to adopt ERM. This leads to a process of lower-level units in an agency leading in implementing ERM and thereby providing good examples for other parts of the agency to follow later.

As John Fraser explained to officials of the US Office of Management and Budget in his 2013 briefing, two essential components of ERM can be described as “conversations” and “prioritization.” The Chief Risk Officer (CRO) is responsible for generating conversations about risk in the agency; a top-level Risk Management Committee is responsible for helping the agency leadership to prioritize risks so that the agency can allocate its scarce resources (funding, staff support, management attention) to addressing the highest-priority risks. Eliciting information about an array of major risks from across the organization allows the agency leadership to gain a view of the portfolio of significant risks rather than neglecting some in a more haphazard approach (See, e.g., Stanton, 2017).

To be most effective, the Chief Risk Officer (CRO) should report directly to the agency head or deputy. When supported by the agency leadership, the CRO then can wield influence without applying formal authority to coerce compliance. The CRO can elicit information, create a supportive network within the agency, and help guide the allocation of resources as a positive rather than negative action, so that units that report major risks become eligible for increased resources needed to bring a risk in line with the agency’s appetite for taking such risks. It has been the present author’s experience that a lack of formal power often can serve as encouragement for unit heads and others to share information with less fear of possible retribution than if they were to share information with a more powerful figure in their hierarchy.

Ideally, the Risk Management Committee also should possess influence without direct authority. That means that the Risk Management Committee should serve as an advisory committee to the agency head or deputy rather than itself possessing authority to make decisions. This allows the agency head to benefit from the risk committee without creating another level of bureaucracy within the agency’s hierarchy. Although the Risk Management Committee may vote as a part of its process of deliberating and prioritizing risks, the agency leadership will benefit more from hearing the deliberation to understand the contours of risk-reward trade-offs rather than be persuaded solely by the results of the voting that may take place.

The Risk Committee Charter needs to fit the agency’s culture. The following topics might be included: (1) overall purpose, (2) scope of deliberations, (3) top-level sponsor, (4) membership, (5) roles, (6) reporting, (7) frequency of meetings/attendance, and (8) the process for making recommendations.

There is an important third element that might be added to “conversations” and “prioritization.” That is implementation. Once the agency’s leadership makes a decision about which risks to address, and how, then the decision must be implemented. The CRO does not manage risk. Rather, it is the responsibility of the head of an organizational unit where risk resides to manage the risk. It is the unit head, rather than a CRO or other official from outside the unit, who best understands the contours of a risk and how best to implement the agency’s decisions about risk. The CRO is responsible for monitoring progress in addressing the risk and in reporting back to the risk committee on progress and possible adjustments that may be called for.

Working together, the CRO and risk committee can help build a constituency for ERM throughout the agency. By creating a network of risk-aware officials, the CRO and risk committee not only gain access to useful information, but also help to encourage the process of cultural change needed to build ERM into decisions and processes throughout the agency. It is most important to create a sense that sharing information about major risks is simply the way that the agency does business, rather than an act of personal courage by someone lower in the hierarchy who dares to bring bad news to his or her superiors.

ERM is a process that each agency needs to adapt to its own culture and needs. This can be done in a variety of ways. For instance, in one federal agency the senior management official, a career executive, has commissioned two years of courses on ERM taught by a local university. In total perhaps 150 staff, including senior executives and the most promising top-level career staff, have undergone training and hands-on exercises in ERM, and further training is being planned.

The agency currently lacks a permanent head and it remains to be seen how the senior management official plans to expand and elevate the current ERM function in the hierarchy. The agency issued the following plan for the establishment of the ERM function over several years:

* “Establish a baseline of common understanding of modern Risk Management principles and nomenclature with a cadre of agency staff from across the agency’s current risk management activities.
* “Form a working group to develop a POA&M (Program of Action and Milestones) to enhance Risk Management at the agency from the trained cadre.
* “Conduct a baseline assessment of Headquarters and Field risk management, oversight, and compliance assurance functions;
* “Identify barriers, gaps, fragmentation, overlaps, and duplication hindering the ability to manage risk from an Enterprise perspective;
* “Identify alternatives for an integration of information to report/monitor comprehensive, current, coordinated, and risk management information for the agency’s Leadership;
* “Assess the gaps, fragmentation, overlaps, and duplication in the current risk management functions of the agency and identify alternatives to continue to mature the risk management function of the agency in support of leadership priorities and strategies
* “Develop a Program of Action & Milestones to enhance Risk Management at the agency by March 2019 (In time to be incorporated into FY2020 Budget Development).
* “Establish performance measures to assess the effectiveness of the agency’s risk management”
* “Recommended courses of action will be presented to senior leadership with corresponding feasibility analyses for decision. The course of action development process will involve multiple reviews with the agency’s leadership at key decision points.”

This agency has designated an accountable risk official, established a small risk staff, set performance goals and a timeline for bringing the ERM initiative to the senior agency leadership, and is building a network across the agency and in the field to help turn ERM into a working reality once the agency leadership signs off.

1. Institutionalizing ERM in an Agency

Once an agency accepts ERM as a process that adds value to performance and decision making, it is important to institutionalize and make it more systematic. Douglas Webster, the first President of AFERM, prepared the following training slide that reflects his approach to establishing and institutionalizing ERM at a federal agency. Nancy Potok, former Chief Operating Officer of the Census Bureau, estimates that it may take perhaps five years to address internal inertia and resistance and make ERM an integral part of the way an agency does business.



Source: Douglas W. Webster, “Enterprise risk management Notional Plan,” George Washington University Center for Excellence in Public Leadership, 2018.

**Exhibit 2: Implementing ERM at a Federal Agency**

As ERM becomes more established in an agency’s way of doing business, next steps involve integrating ERM into a range of agency processes. A 2019 AFERM survey of participating agencies indicates that an especially important step is to include risk management in performance plans of senior executives. Useful performance criteria for officials at all levels might include whether they (1) support performance of the agency as a whole and not just of their particular unit, (2) collaborate well with others, (3) promptly bring “bad news” to relevant decision makers (and the CRO), and (4) give and take feedback graciously.

Another useful step is to require that all major proposals include a discussion of (1) major risks and (2) how they will be addressed. Too often agency officials bring proposals to their superiors, emphasizing the valuable results that could come from implementation. Such proposals would become stronger, and more reassuring to agency leaders, if they included explicit recognition of major risks and why the risk-reward trade-off has value.

Finally, ERM is strengthened to the extent that it is incorporated into agency budget processes and strategic plans. The agency Chief Financial Officer can be an especially influential supporter of ERM. Many CFOs not only take an enterprise-wide view of resource allocation for their agencies, but also have a good view of multi-year developments. To address a major risk early, and thereby forestall the need for spending many more resources later, is something that fits nicely within the skill-set and perspective of a good CFO. Similarly, although government strategic planners may lack the influence of a CFO, they can strengthen their plans by including a discussion of risks that could affect the agency’s ability to achieve its goals and objectives.

**Differences between ERM in Government and ERM in a Private Company**

In legal terms, the fundamental difference between a government agency and a completely private company is that a private company (with notable exceptions not relevant here) may engage in any activity except where prohibited by law. By contrast, the government agency may engage in only those activities that are authorized by law. Thus, while the leader of a private company has considerable discretion in hiring, promotion, and firing of employees, those actions are tightly constrained by law for a government agency. Similarly, the private company can select the lines of business in which it wishes to engage, while the law specifies the mission of a government agency and the activities in which it must engage and those in which it may not. Perhaps most importantly, for the private company revenues tend to be linked with the volume of goods or services it provides; for the government agency budgets for staffing and investments may be completely disconnected from the budgets that fund the actual goods or services that the agency provides. Exhibit 3 summarizes some of the organizational differences. (For a more complete discussion, see e.g., Stanton 2006).

|  |  |
| --- | --- |
| **Government Agency** | **Ordinary Company** |
| Political factors predominate; the market affects some agencies, especially government corporations | External environment is more market-based than political |
| Subject to controls on resources that often include annual appropriations limits; a tendency exists to maintain agency functions despite inadequate resources or capacity  | Stream of profits generates needed resources to build capacity |
| Accountable to multiple parts of government and, in varying degrees, to influential constituencies | Accountable to private owners |
| Some public disclosure; often less financial disclosure than is required for private firms | Financial disclosure to private owners; if a publicly held firm, also required public disclosures |
| Heavy controls on inputs (e.g., budget and staffing) and procedures; government corporations may have greater autonomy | Market-based external controls based upon financial performance  |
| Diffuse political pressures lead to serving multiple purposes that often may not be articulated | Profit-oriented goals may force focus upon particular activities, market segments and strategies |
| May stagnate over time, as public priorities change, without ceasing to exist | Life cycle: thrives or goes out of business; forced exit of failed firms |

**Exhibit 3: Differences in Resources, Flexibility, Environment, and Life Cycle:**

**Government Agencies and Ordinary Private Companies**

There are also significant risk management differences between the two organizational forms. While strategic risk is associated with many large private company setbacks or failures (e.g., Barber et al., 2019), federal agencies such as the US Postal Service may be confined to their traditional roles long after market and technology developments have made their primary purposes obsolete. Reputational risk does affect both private and government organizations, but the structure of congressional oversight tends to make hiding untoward circumstances much harder for a government agency than for a private company. Finally, a government agency could be more prone to suffer what might be called capacity risk, i.e., a large disparity between funding for administrative structure vis-à-vis the volume of goods or services the organization is expected to provide. One could conjecture that capacity risk in turn relates to greater operational risks, and greater incidence of failures, at a federal agency than at a private company. However, absent careful analysis, that would be difficult to substantiate.

ERM practice also can differ between the public and private sectors. This can be seen in the practice of determining an organization’s risk appetite. In contrast to private companies that might keep their risk appetite statements confidential within the organization, federal agencies are sensitive to the way that the Congress might characterize a risk appetite statement that reflects practical reality rather than more ideal circumstances. Consider, for example, the following risk appetite statement of the Office of the Comptroller of the Currency (OCC), supervisor of national banks:



**Exhibit 4: Office of the Comptroller of the Currency’s Statement of Risk Appetite**

Source: Office of the Comptroller of the Currency, Enterprise Risk Appetite Statement, April 2016

The statement includes definitions of the terms “low” and “moderate,” and of the risk categories. Note that, unlike risk appetite statements from the corporate world, the OCC presents no areas where a high appetite for risk would be acceptable. To some extent this reflects the OCC’s organizational culture: an agency carrying out essentially an audit function tends not to like to take risks. In addition, federal agencies must consider the political context of any reports they prepare. Congressional scrutiny could follow any admission that an agency is willing to take any large risks, or even smaller risks in a category such as fraud, where it can be politically unacceptable for the agency to admit that it accepts or expects any fraud at all.

There are other differences between the sectors as well. Private companies often have access to a greater volume of resources for information technology than do federal agencies. This allows private companies to rely more heavily on quantitative risk modelling than is possible in most of government. Moreover, government can be subject to many of the types of nonquantifiable risk that can affect a private company, and also to essentially random major risk events such as whether the United States Congress may delay or fail to appropriate funds for a government agency’s operations in any particular year.4

Finally, there is the matter of risk governance. Private corporations are governed by boards of directors that, in concept at least, are supposed to have a fiduciary responsibility to protect the interests of shareholders. That responsibility tends to lead to selection of company officers and staff whose qualifications relate to the positions that they hold. (See, e.g., Stanton, 2012). By contrast, heads of government agencies may on occasion possess few if any qualifications, other than perhaps political acumen, relating to the positions that they hold. Again there are significant counter-examples. One factor that tends to impede consistent application of ERM in a government organization relates to the speed with which political appointees may rotate into and out of their plum government positions. As the following section explains, this type of instability makes it useful for ERM to spread across government as a matter of cultural change rather than merely because a particular agency leader might promote ERM as a way to protect his or her reputation from an adverse event if an otherwise unexpected major risk were to cause significant harm.

**Unusual Characteristics of the Governance Framework of the United States**

Establishing ERM in the US federal government has had reverses as well as successes. The Defense Logistics Agency (DLA) established a leading ERM program when a new agency head called for it. Then the officer rotated to a new position in the defense establishment, followed by a successor agency head who lacked interest in ERM. The CRO office was layered under a deputy CFO and languished. The very capable CRO left for another federal agency. Then yet another high-ranking officer became head of DLA and is presently restoring ERM again to be a significant part of DLA processes. (Personal communication to the author, June 2019). ERM at other agencies sometimes has undergone similar swings from being a core part of decision making to leadership disinterest, and sometimes back again. Fortunately, the ERM network represented by AFERM and other nonprofit, governmental, and private organizations, continues to grow in strength and influence as ERM spreads to an increasing number of agencies.

This is quite different from the top-down approach taken by governments in the United Kingdom or in Canada, Australia, or other parliamentary systems based on a tradition of “peace, order, and good government.” These countries tend to impose ERM, or “integrated risk management” as it is also known, much more directly than in the US. (For a history of ERM in those countries, see, e.g., Stanton, 2015). Thus, the 2020 UK *Orange Book on Management of Risk – Principles and Concepts*, issued by H.M. Treasury, sets forth guidance on risk management in a way that differs significantly from the efforts of the US Office of Management and Budget to encourage rather than mandate ERM. By contrast to the current US approach, the UK *Orange Book* (p. 3) requires government organizations to comply with the guidance or explain why not:

“Each government organisation is required either to disclose compliance or to explain their reasons for departure clearly and carefully in the governance statement accompanying their annual resource accounts. The requirement for an explanation allows flexibility, but also ensures that the process is transparent, allowing stakeholders to hold organisations and their leadership to account.”

The network-based approach to bringing ERM to federal agencies responds to unusual institutional characteristics of the US government. The United States government, as established by the US Constitution, differs fundamentally from the structure familiar in the United Kingdom, Canada, or Australia. As Richard Stillman points out in his insightful book, *Preface to Public Administration* (1991), the US began as a group of colonies which resented being subject to a very effective imperial administrative apparatus. In consequence, the framers of the US Constitution placed great emphasis on checks and balances and distributed power within government and among levels of government. They created,

“…a national political community…without an administrative state… America was formed . . . not only without a state, but with a hodgepodge of competing beliefs, doctrines, principles, myths, and postulates, often in conﬂict with one another, that ... serve to continuously pulverize administrative effectiveness and to negate possibilities for any consistent administrative design.” (Stillman, pp. 27, 33)

Under this system, while the President of the United States can serve as a centralizing figure to promote common administrative practices across government, the Congress is an off-setting centrifugal force that tends to create disparate administrative cultures at each agency. The iron triangle of agencies, their interest groups, and their congressional committees, results in a wide variation in organizational capacity and management quality across the federal government. On the other hand, while a US federal agency may be subject to more frequent changes than in a parliamentary government, agencies also tend to be open to considering new management approaches such as ERM. This has been seen in a range of management changes over the years that have improved the way that agencies carry out their work. One important consequence of the US governmental structure is that an emphasis on creating a network of practitioners and a constituency for ERM seems far more promising than relying only on trying to dictate the practice of ERM from the top down

**Next Steps for ERM in the US Federal Government**

ERM continues to expand in the federal government. Next steps are likely to include: (1) building skills of collaboration, reporting bad news to those who need to know, and giving and taking feedback graciously into the personnel requirements for senior executives and other career civil servants, and (2) systematically including considerations of major risk into the annual budget process. Ideally, an agency, as a part of its budget review at the Office of Management and Budget, would flag major risks that could affect achievement of its objectives and suggest how additional resources might be wisely spent to address them in a cost-effective way. At a time of constricting budgets for many agencies, there is some evidence that a fact-based and supportable analysis of risks can persuade policymakers not to make some of the cuts that were initially intended. This is the type of flexible and durable approach that can allow ERM to become an integral part of the way that the US federal government does business.

**NOTES**

1. The author wishes to thank David Fisher, Sallyanne Harper, and Douglas Webster, for their contributions to this chapter. The author remains solely responsible for any errors or omissions.
2. In the US government the term agency denotes generally large organizational units that may or may not be constituent parts of a larger federal cabinet department.
3. The first practitioner of ERM in the federal government, Stanley M. Dore III, who came from the financial sector to establish a risk office at the Office of Federal Student Aid in 2005, was a member of the original group of seven officials.
4. It is useful to distinguish the idea of “risk,” defined as an event with incidence and severity that are susceptible to quantification, from the idea of “uncertainty,” which is not quantifiable. (Knight, 1921). While all organizations are subject to uncertainty, a government agency often seems subject to a much higher degree of uncertainty than a private company.

**REFERENCES**

**Government Documents**

HM Government. (2020). *The Orange Book: Management of Risk – Principles and Concepts*. HM Treasury: Government Finance Function.

Internal Revenue Service. (2017). *Form 1023-EZ Update Report*. Washington, DC. Available at https://www.irs.gov/pub/irs-tege/form\_1023ez\_update\_report\_final.pdf.

Office of Management and Budget. (2016). OMB Circular No. A-123, “Management’s responsibility for enterprise risk management and internal control,” Washington, DC. July 15. Available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf.

Office of the Comptroller of the Currency. (2016). “Enterprise Risk Appetite Statement,” Washington, DC: April.

United States Chief Financial Officers Council and Performance Improvement Council. (2016). *Playbook: Enterprise risk management for the US Federal Government*. Washington, DC. July 29. Available at https://cfo.gov/wp-content/uploads/2016/07/FINAL-ERM-Playbook.pdf.

**Books**

Fletcher, K.C., and Stanton, T.H. (2019). *Public Sector Enterprise risk management: Advancing Beyond the Basics*. New York: Routledge.

Hardy, K (2015). *Enterprise risk management: A Guide for Government Professionals*. San Francisco, CA: John Wiley & Sons, Inc.

Knight, F.H. (1921). *Risk, Uncertainty and Profit*. Boston, MA: Houghton Mifflin and Co.

Stanton, T.H. (2012). *Why Some Firms Thrive While Others Fail: Governance and Management Lessons from the Crisis*. New York, NY: Oxford University Press.

Stanton, T.H., and Webster, D. W. (2014). *Managing Risk and Performance: A Guide for Government Decision Makers*. Hoboken, NJ: John Wiley & Sons, Inc.

Stillman, R.J. II. (1999). *Preface to Public Administration: A Search for Themes and Direction*, Second Edition. Burke, VA: Chatelaine Press

**Other Readings**

Barber, F., Whitehead, J., and Bistrova, J. (2019), “Why giants stumble,” *California Management Review*, Vol. 62 (1) 5–30, November.

Fletcher, K.C. (2019). “Change management and developing organization risk culture: Transportation Security Administration case study,” chapter 2 in Fletcher, K.C., and Stanton, T.H., eds. *Public Sector Enterprise risk management: Advancing Beyond the Basics*. New York: Routledge.

Rappeport, A. (2017). In targeting political groups, I.R.S. crossed party lines. *New York Times*. October 5.

Stagnitti, J. (2014). “Integrating enterprise risk management with strategic planning and resource management,” chapter 8 in Stanton, T.H., and Webster, D. W., eds. *Managing Risk and Performance: A Guide for Government Decision Makers*. Hoboken, NJ: John Wiley & Sons, Inc.

Stanton, T.H. (2006). “Moving toward more capable government: a guide to organizational design,” chapter 1 in Stanton, T.H., ed., *Meeting the Challenge of 9/11: Blueprints for More Effective Government*. Armonk, NY: M.E. Sharpe, Inc.

Stanton, T.H. (2015). “The growing movement for enterprise risk management in

government: the United States begins to catch up,” *Asia Pacific Journal of Public Administration* 37(3), pp. 182-192.

Stanton, T.H. (2017). “An Agency Guide for ERM Implementation,” Association of Government Accountants, available at, https://www.agacgfm.org/Research-Publications/Online-Library/Research-Reports/An-Agency-Guide-for-ERM-Implementation.aspx

Stewart, M.G., and Mueller, J. (2016). “Risk and economic assessment of expedited passenger screening and TSA PreCheck,” *Journal of Transportation Security*, 29 Nov.

Vetrano, F. and Stayanovich, J. (2019). “Using data and analysis to add value from ERM,” chapter 3 in Fletcher, K.C., and Stanton, T.H. eds., *Public Sector Enterprise risk management: Advancing Beyond the Basics*. New York: Routledge.

**Multimedia Presentations**

Mikes, A. (2010). "Enterprise risk management at Hydro One (Multimedia)." Harvard Business School Multimedia/Video Case 110-707, June.

Potok, N. (2015). “US Census Bureau enterprise risk management program operationalizing ERM – a top-down, bottom-up approach.” US Census Bureau.

Webster, D.W. (2018). “Enterprise risk management notional plan.” George Washington University Center for Excellence in Public Leadership

**ABOUT THE AUTHOR**

**Thomas H. Stanton** is a former President of the Association for Federal Enterprise Risk Management (AFERM) and a former member of the federal Senior Executive Service. He served for many years as a board member of the National Academy of Public Administration (NAPA), and as Chair of the NAPA Standing Panel on Executive Organization and Management. In 2017 NAPA honored him with the George Graham Award for Exceptional Service to the Academy. In 2018 AFERM honored him with the Enterprise Risk Management Hall of Fame award. Mr. Stanton teaches as an adjunct faculty member at the Center for Advanced Governmental Studies at the Johns Hopkins University. His publications include two co-edited books on ERM in the US federal government, *Managing Risk and Performance: A Guide for Government Decision Makers* (Wiley, 2014), and *Public Sector Enterprise Risk Management: Advancing Beyond the Basics* (Routledge, 2019). His book *Why Some Firms Thrive While Others Fail: Governance and Management Lessons from the Crisis* (Oxford, 2012), builds on his service with the Financial Crisis Inquiry Commission. Mr. Stanton holds degrees from the University of California at Davis, Yale University, and the Harvard Law School. Further information can be found at [www.thomas-stanton.com](http://www.thomas-stanton.com).