CliftonLarsonAllen

The Strategic Value of Enterprise Risk Management for Federal Agencies

Two representative agencies illustrate the power of ERM in planning and policy making

Federal agencies tend to think of enterprise risk management (ERM) as something that is only useful in the private sector. But risk is everywhere. Like commercial enterprises, federal agencies face threats every day — to their finances, reputation, strategic mission, and operational effectiveness. ERM is about identifying, analyzing, and addressing those risks. There are key differences in the application of ERM in federal agencies versus the private sector, but it can still be a powerful resource for strategic planning and effective policy making.

Introduction

The federal government faces unprecedented fiscal challenges. The economic downturn, slow recovery, political gridlock, and federal fiscal sustainability issues have created the highest risk environment since the Great Depression. For evidence we need only look at recent events.

- The failure of Congress to approve a budget led to a temporary government shutdown and fixed, across-the-board spending cuts.
- Multiple debt limit crises, in which Congress has only agreed to meet the full fiscal obligations of the nation at the very last minute.

- The 2008 mortgage crisis, which led to the institution of the Troubled Asset Relief Program (TARP), requiring more than $460 billion of capital infusions, guarantees, and loans to stabilize the financial system.

Enterprise risk management

While federal agencies cannot stabilize the political system or the financial markets they can develop an effective approach to identifying, measuring, and assessing risks and developing effective policy responses. Enterprise risk management is such an approach.

The Committee of Sponsoring Organizations (COSO) calls ERM a process for identifying potential events that could affect an organization, and then taking steps to reduce or eliminate the risk so the organization can achieve its objectives.

This definition assumes that by proactively addressing risk and understanding its likelihood and magnitude, an organization can create value for its stakeholders and make sound resource allocations.

ERM is different for federal agencies

Business oversight and governance are different in the federal sector. For example, in the private sector, access to private capital markets, profitability, and shareholder return on investment are key concerns that keep CEOs up at night. But in the federal sector, top-of-mind issues include legislation that reduces appropriations, decreases tax revenue, and imposes congressionally mandated spending cuts. Rather than shareholders, the stakeholders of federal agencies are legislative and executive officials who authorize funding as well as the public that is dependant on government services.

Since the federal government has the power to tax and borrow from the capital markets, its agencies have not traditionally had the short-term liquidity pressures of the private sector. But today the federal government also faces liquidity pressures as it struggles to meet the rising costs of Medicare, Medicaid, Social Security, pensions, and services for a growing population.

Another major challenge is the vast array of laws and policy regulations imposed on federal agencies. From the financial reporting regulations and internal controls required by the Office of Management and Budget, to complex appropriations laws, federal government administrators face a constant uphill battle.

The impact of failure in the federal government, or even poorly optimized resources and programs, is also huge. With a budget of more than $1 trillion and more than 4 million civilian and military employees, government touches virtually every aspect of the lives of 310 million citizens. While a security breach at a Fortune 1000 manufacturer may put thousands of individuals or businesses at risk for fraud, a similar breach at a major intelligence agency could imperil the security of the nation.

An ERM framework and case study

The ERM framework for a federal agency is the same as it would be for a commercial, state, or local organization, except the structure of risk must account for the regulatory structure in place, and impacts must be assessed more broadly for the economic footprint of the federal government.

To understand the complex nature of federal government, let's look at two representative agencies:

- A Department of Defense agency with weapons systems that extend over long life cycles, a substantial civilian and military workforce, extensive dealings with outside contractors, and worldwide operations.
- A civilian agency that makes benefit payments to a large number of constituents, has diverse geographic operations, a large civilian workforce, and is highly dependant on information systems to carry out its mission.

To use this ERM framework we had to establish how likely it would be for certain risks to create monetary or credibility damage to the federal government. The framework is then used to assess the consequences of an unaddressed risk. All of the risks are combined for an overall rating, which is then applied to each of the major departments in the agency and to the agency's capital program.

The six-stage ERM process

Implementation of an ERM initiative in a federal agency follows a process that is similar to a commercial enterprise, although the scope of the risk is much broader. The process proceeds through six stages.

Step 1: Establish the risk types

Some ERM models concentrate on a few limited areas. In the federal government, a broad array of risks must be considered. Each risk in our case study is assessed and described in Chart 1.

Step 2: Define the likelihood and impact of risks

In our case study, risks were categorized by their likelihood and impact, and the nature of the assessment was defined. For example, a taxation and budget risk was assessed on the funding in jeopardy compared to the overall budget, while intergovernmental risk was defined by the degree to which the agency interacts with other federal agencies for services and payments.

Chart 1: Risk Types Used in Model

LIKELIHOOD		IMPACT	
Taxation and Revenue Risk	Assessed on the basis of level of expenditure at risk compared to the president's overall budget.	Reputation or Public Perception Impact	Assessed by determining risk that the agency suffers a diminished reputation or public perception from a risk occurring.
Intergovernmental Risk	Assessed by the degree to which the department is dependent on timely receipt of funds and services from other federal agencies.	Business Operations Impact	Assessed by looking for impacts occurring that lead to ineffective or inefficient agency operations or not meeting internal or external goals. This could include failures from changes in the volume or complexity of transactions or activities.
Public Policy Risk	Assessed by the degree to which political pressure at the congressional level could alter existing plans at the department level. For instance, the Department of Defense may have a major weapons program in process that needs to be delayed or modified due to sequestration.	Financial Reporting and Operations Impact	Assessed by significant financial implications to the department or agency, such as financial misstatements or failure to meet financial obligations.
Strategic Risk	Assessed as the inability to meet business objectives and strategies due to improper or unfocused strategic planning, an inefficient organizational structure, or an ineffectively applied or inefficient business model.	Economic Impact	Assessed by significant reductions in economic outcomes to the nation such as gross domestic product or the levels of employment or inflation.
Financial Operations Risk	Assessed by determining the quality of accounting and budget information and whether it of sufficient quality to ensure that key financial operations such as revenue collection and financial reporting function properly.	National Defense and Security Impact	Assessed by significant reduction in the scope and/or quality of the nation's defense systems, capabilities, and infrastructure.
Information Technology Risk	Assessed by determining if the technology the agency uses effectively supports its operation, and whether its systems are opens to compromise or illegal access.	Public Policy Execution Failure	A measure of the failure of public policy to be executed for lack of funding. Enviromental impact from lack of enformcements would be an example.
Legal and Regulatory Risk	Assessed by determining if the agency complies with all major federal laws.		
Integrity and Fraud Risk	Assessed by reviewing the actual instances of waste, fraud, and abuse that have been documented in recent years, and by assessing vulnerabilities in operations such as exposure to cash collection or inadequate segregation of duties.		
Customer Service and Delivery Risk	Assessed by how well the agency delivers its services. Considers the risk that a department may be susceptible to not serving customers in a timely and effective fashion.		
Environment, Health, and Safety Risk	Assessed by looking for conditions or vulnerabilities that can have an adverse effect on the environment or that threaten the health and safety of communities.		
Human Resource Risk	Assessed by determining if the agency workforce has the proper skills sets, resources, and training to complete its missions, and whether its level of benefits is sufficiently competitive to attract a strong workforce.		
Information and Communication Risk	Assessed by determining if there is consistent, accurate, and timely communications to internal and external constituencies.		
Overall Likelihood Risk	A blend of the 12 factors weighted and tempered by judgment.	Overall Impact Risk	A blend of the six factors weighted and tempered by judgment.

Step 3: Define the level of risk intensity
A heat map was created to indicate the intensity of risk. Chart 2 uses a five-point scale that includes very high (VH), high (H), moderate (M), low (L), and very low (VL).

Chart 2: Level of Risk Intensity

LIKELIHOOD		IMPACT
An immediate and high degree of vulnerability such that it is critical that the risk be managed and controlled in order for this area to achieve its objectives. If not properly controlled, this area could have a serious, long-term or detrimental effect on operations, internal controls, and the achievement of organizational goals and objectives.	VH	If an event occurs, the financial ramifications would be severe and/or operations would suffer long standing consequences.
A less immediate and somewhat lower degree of vulnerability such that it is important that the risk be managed and controlled in order for this area to achieve its objectives. If not properly controlled, this area could have a significant, long-term, or detrimental effect on the organization	H	If the event occurs, the financial ramifications would be signficiant.
The risk present should be addressed and controlled, but the probability is not as severe as defined above. If not properly controlled, the area could have some impact on operations and internal controls, but organizational goals and objectives will still be met.	M	Indicates that the resulting consequences of an event would be negative and must be managed, but would not have a substantial effect on finance or on-going operations.
A serious event is possible. The area should be managed but the level of risk response is limited.	L	Indicates that the event occurring would have a small impact financially or operationally.
The threat of a serious event is either non-existent or remote. The area should be managed but the level of risk response is limited.	VL	Indicates that the event occurring would have little or no impact financially or operationally.

Step 4: Surveying and interviewing managers
One of the best ways to develop the intensity ratings for the heat map is to survey senior and upper mid-level managers who are close to operations. In our case study, both agencies surveyed top and middle managers in all departments. We also reviewed budgets, financial information, and audit reports before interviewing government officials

The survey was distributed to 150 managers. Questions covered the major risks to the agency, and included pre-testing with selected employees. Ratings were assigned for each question and data were compiled from department responses and compared to an overall average. The results were used to score and map risks by category and department. Interviews yielded information about departmental context, specific risk areas, and the overall risk environment.

Step 5: Develop a visual summary
Risk maps were completed using both the survey and interview results. The risk map (Chart 3) displays the intensity of each risk as developed in step 4 using the very high (VH) to very low (VL) scale for each type. A rating was then assigned for each type (i.e., taxation and revenue risk or intergovernmental risk).

Chart 3: Summary of Assessed Risk for Each Agency

		Defense Agency	Civilian Agency	Reason For Assessment
LIKELIHOOD	Taxation and Revenue Risk	VH	H	In the current environment, 50 percent of the cuts from sequestration accrue to defense agencies that have 17 percent of the overall federal budget. So risk is higher in the defense agency.
	Intergovernmental Risk	VH	H	The defense agency deals with more Department of Defense entities than does the civilian agency and the complexity results in slightly higher risk.
	Public Policy Risk	VH	VH	Both entities face high levels of congressional pressure that could upset long-range plans and budgets.
	Strategic Risk	VH	H	The defense agency has more long-term expenditures and a more complicated structure of intergovernmental relationships, so its strategic risk is higher.
	Financial Operations Risk	H	VH	The civilian agency needs to carry out many more transactions related to benefit delivery and the volume of these transactions increases its financial operations risk.
	Information Technology Risk	VH	H	The dependence on information systems is high at both agencies, but the intensity of risk in a national security environment is greater.
	Legal and Regulatory Risk	M	VH	The civilian agency is subject to more laws and regulations.
	Integrity and Fraud Risk	M	H	Both agencies have tight controls over operations and workforces that are in many cases subject to security clearances which lessen the risk of fraudulent behavior. Each has active inspector general offices. The civilian agency has a greater chance of making improper payments, which result in its higher rating.
	Customer Service and Delivery Risk	L	H	The risk is higher at the civilian agency since there is a high level of customer interaction in the benefits area.
	Environment, Health, and Safety Risk	L	L	Neither agency has extensive operations with environmental impact.
	Human Resource Risk	H	H	The risk is high at both agencies as the impact of austerity programs dilutes both training and benefits.
	Information and Communication Risk	H	H	Communication with internal and external constituencies is important at both agencies.
	Overall Likelihood	VH	H	A judgmental blend was made.
IMPACT	Reputation Impact	VH	VH	Both agencies have high reputational risk since their impact to the country is so pervasive.
	Business Operations Impact	M	VH	The risk rating of the civilian agency is higher since the operations of the civilian agency are larger.
	Financial Impact	VH	VH	The risk of insufficient funding and all its ancillary effects are very high at both agencies.
	Financial Reporting and Operations Impact	H	H	Neither agency has investors as an organization would in the private sector, so the risk of financial misstatements has less financial impact than it woiuld for a publicly traded firm.
	Economic Impact	VH	VH	Both agencies expend tens of billions of dollars, so their impact on the economy eclipses all but the very largest private entities.
	National Defense and Security Impact	VH	L	As expected, the defense agency has a much higher impact from risk in this area.
	Overall Rating	VH	VH	A judgmental blend was made.

Step 6: Synthesize the results

Here is where the power of the ERM model and the heat map becomes apparent. The likelihood and impact risks are high for both agencies, but the component risks leading to that assessment are very different. At the defense agency, the higher level of funding risk, complexity, and reliance on information systems drives taxation and revenue, intergovernmental, strategic, and information systems risks. On the impact side, national security risk is far higher at the defense agency. The higher level of transactions and improper payment risk of the civilian agency, and its exposure to more regulations, drive its higher ratings for financial operations and integrity/ fraud risks.

Applying the ERM model

Decisions involving audits, budgets, and strategic plans can all benefit from an ERM assessment. The results can be used to develop a multi-year internal audit plan that concentrates resources on the highest risk areas, and can also be a tool for developing and validating multiple budget scenarios reflecting the changing levels of congressional funding. Agencies can create alternative budget scenarios to account for projected lower appropriations, potentially higher employee turnover, and greater risk in implementing programs over time.

Agencies can also address risk in the strategic planning process, making risk consequences and trade-offs transparent among departments. Survey and interview results also help management focus on risk in areas where they may not have done so before.

In an era of increased risk, ERM helps federal agencies make important policy decisions based on proactive assessments of changing circumstances. As executed by a committed, informed senior management team, ERM can also help government leaders make sound resource allocations.

Resources

Author

John E. Homan, Senior Manager, Government Services