

No Surprises. Turning Federal Agency Risks into Opportunities:

An Enterprise Risk Management Approach*

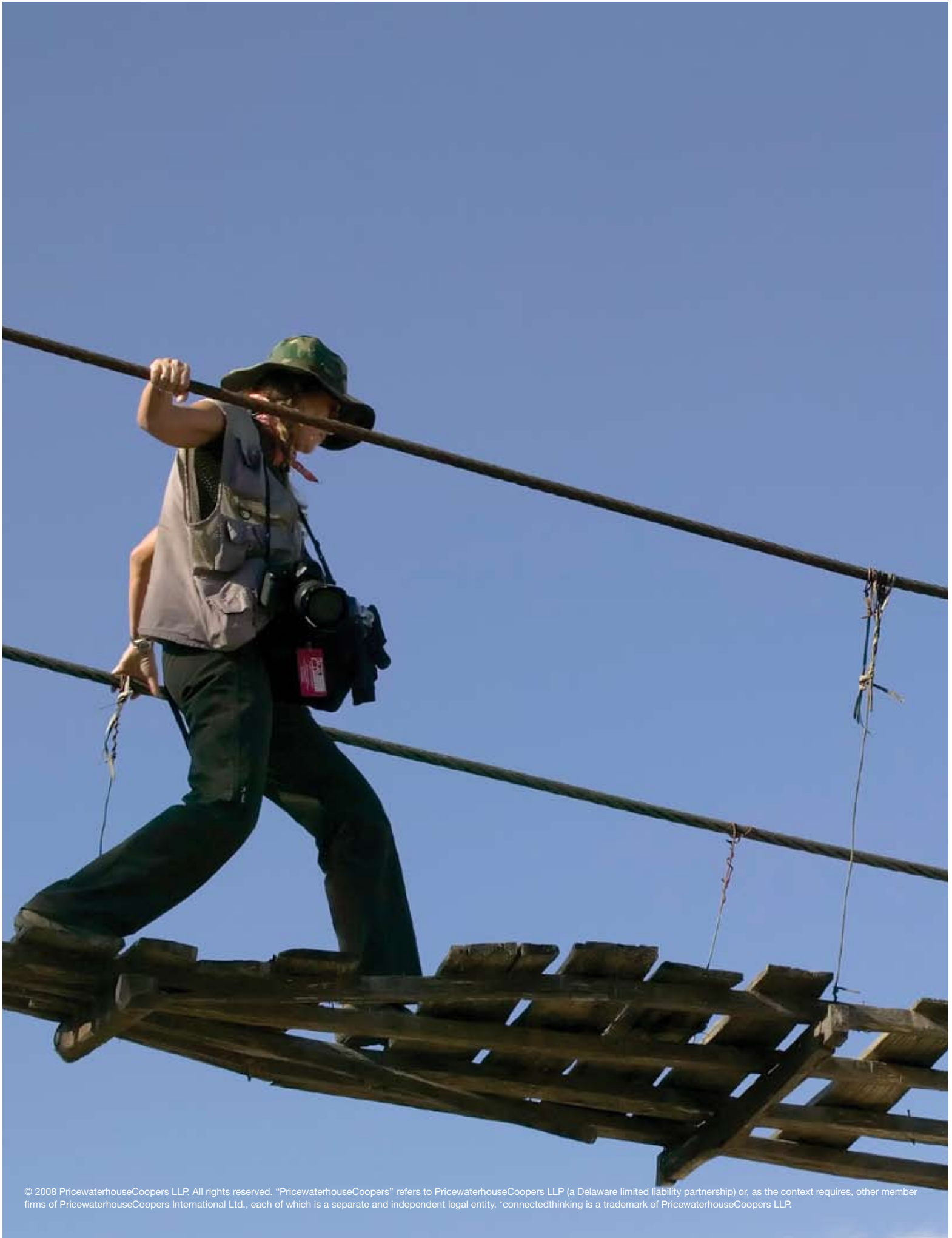
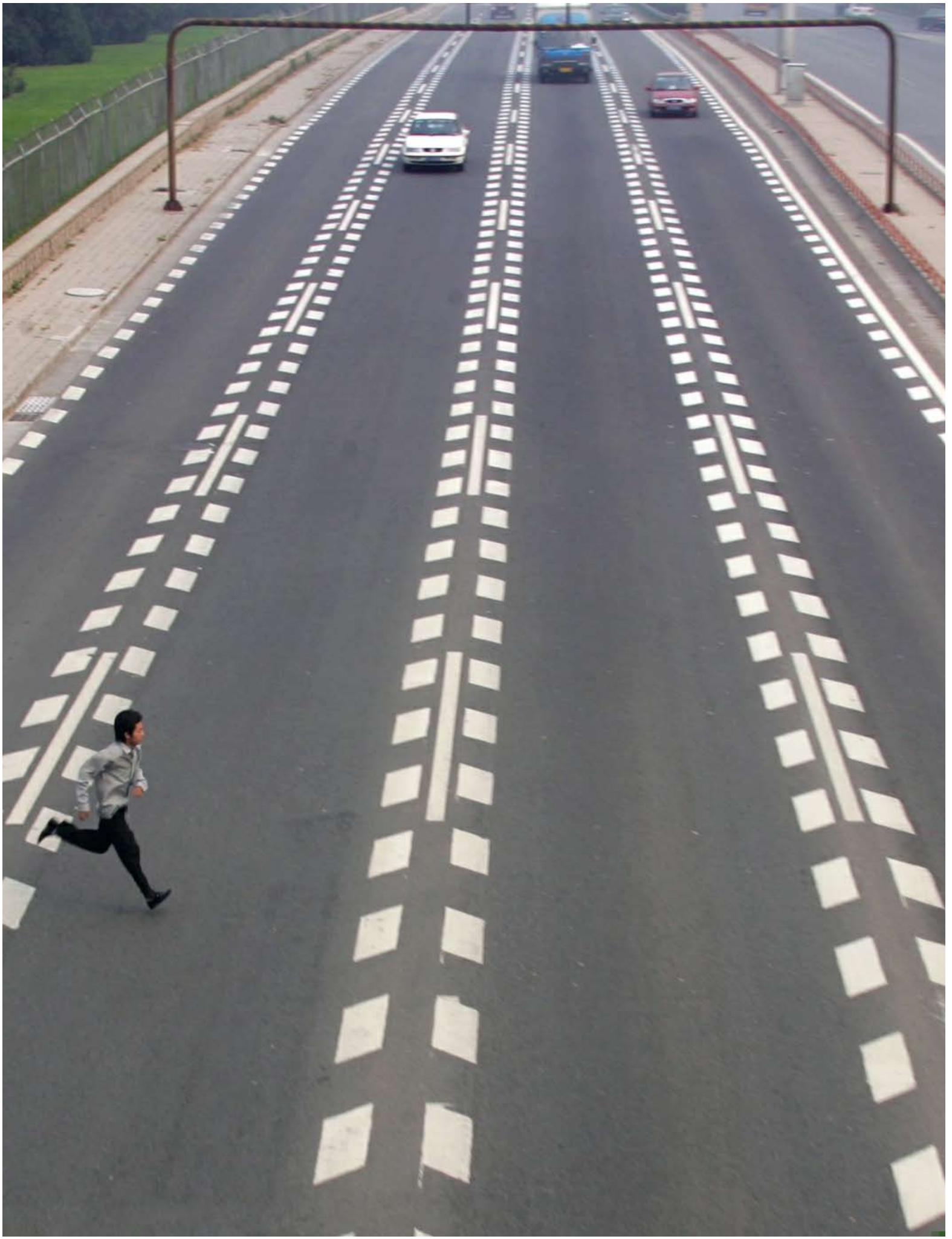


Table of contents

Part 1: Introduction.....	3
Part 2: PwC's ERM Methodology.....	7
Part 3: Achieving ERM Benefits	11
Part 4: Summary.....	16



Part 1: Introduction

Enterprise Risk Management (ERM):

A comprehensive, systematic approach for an organization, to measure, prioritize, and respond to the risks challenging its most critical objectives, related projects, initiatives, and day-to-day operating practices, regardless of the organization's size or mission.

Data is compromised... In the media and on Capitol Hill, the blame game begins. Within the past two years, Federal agencies have been in the public eye, featured within articles and news wires reporting damages that could have been prevented through risk management. One significant risk is the loss of sensitive data. The U.S. Department of Veterans Affairs (VA) and Transportation Security Administration (TSA) have spent many resources responding to these types of issues as outlined in the U.S. Government Accountability Office's (GAO's) report on information security¹ and on TSA's public web page². At VA, a laptop was stolen from an employee nearly 2 years ago containing sensitive information on more than 26 million U.S. military veterans. For TSA, an external hard drive went missing, either as a result of theft or misplacement, with payroll information data on about 100,000 employees. Each of these incidents resulted in a media firestorm and Congressional inquiries. What signals or indicators could have prevented these incidents? Is it even possible to anticipate and mitigate these risks within the normal operations of the agency?

An Enterprise Risk Management Program (ERMP) would have provided the predictors for these risks, and allowed executives to mitigate them. With predictive indicators, such as the number of laptops in the field intersected with the number of employees that have access to sensitive information, VA and TSA will be better prepared to address potential risks early and mitigate their occurrence. For example, with these indicators, VA and TSA could have identified specific laptops or external drives meriting tracking devices. Those devices limit exposure through theft or loss of data.

Though costs are associated with the establishment of controls, the cost savings associated with responding to risks proactively can be measured in dollars and reputation. For TSA, there was not only a cost associated with a damaged reputation in the eyes of the public, but TSA was also impacted financially: they were required to provide the affected employees with identity theft protection and credit monitoring for one year, and they spent time and money responding to inquiries about the control environment around data privacy.

ERM does not prevent all risks from becoming issues. A structured approach to risk management provides an agency with reasonable assurance that indicators and information are made available to the appropriate individuals in order to assist with risk mitigation efforts. This paper discusses the current risk environment with Federal agencies, PricewaterhouseCoopers' (PwC) ERM methodology, and the benefits an agency can realize by implementing an ERMP.

Why Risk Matters: Turning Risk into Opportunity

Senior leadership must assess five key risk areas and act to prepare their agencies for the significant changes they will face over the next decade. In doing so, they must ask: How are we positioned to keep pace and succeed in the future? What risk and control management processes and lessons learned can be leveraged and shared across the agency? How can we instill risk management rigor and discipline to all aspects of our agency? Through an ERMP, these types of questions are addressed through consistent and comprehensive analysis. An ERMP proactively identifies risk and provides an agency with the means to manage risk and generate opportunities by creating options for management. These options help create human capital stability, enhance operational performance, and create an adaptive environment that allows an agency to seamlessly plan for transformation.

¹ GAO Report GAO-08-343, Information Security, Protecting Personally Identifiable Information.

² http://www.tsa.gov/press/happenings/050407_statement.shtm

1 Political Risks

How do senior career staff predict the impact of a changing administration on its ability to operate and manage funding and resources? What planning should occur to minimize the angst associated with the looming election? Are alternate options available? Political risk assessment helps agencies better understand different scenarios to minimize surprises and prepare operations to adapt to a new environment. By integrating political risk into enterprise risk management, agencies can better understand the nature of political risk and its impact on their strategic plan and day-to-day business operations but also realize additional benefits. For example, they are enabled to respond earlier, more flexibly, and more comprehensively to new or changed requirements.

Because Federal agencies are directly impacted by political decisions, the political environment must be factored into strategic planning. Political risk can seem so fluid that many leaders lack a framework for evaluating their exposure. One of the main challenges is identifying the specific indicators of political risk from the overwhelming body of available information. A customized ERM framework helps organize complex, cross-national phenomena into manageable, actionable typologies. Through this framework, an agency is able to measure the business consequences of political risk and obtain an early warning of a problem or opportunity presented by political shifts.

2 Human Capital Risks

Issues relating to human capital are continually being cited as a root cause to many of the issues and challenges facing Federal agencies. In 2001, GAO added Strategic Human Capital Management to its high-risk list, yet agencies continue to struggle with mitigating these risks³. Specifically, agencies are increasingly faced with challenges created by a retiring workforce, decrease in available funding, and knowledge retention. Is capacity building to continue momentum if we do not have funding for contractors? Are processes, SOPs, and training materials documented to mitigate loss of knowledge transfer? In many cases, these questions have been unanswered.

Assessing human capital risk within a standardized ERM framework provides an agency with the information needed to develop a long-term roadmap, integrated into a strategic plan to effectively manage changes within their operational structure. For example, if an agency assesses its workforce and determines staff is eligible for retirement, the agency may reevaluate or develop a strategy for retaining experienced individuals. A procedure requiring the development of succession plans for any eligible retirees may also be created. Standardizing human capital risk management into an ERMP allows an agency to assess the risks within their current Human Capital Environment and predict how today's workforce needs to adapt to tomorrow's needs.

3 Information Technology Risks

Rapid technological advances over the last several years have expedited the pace of business. As the rate of change accelerates, management must anticipate and focus on allocation of resources to drive business performance. Many Federal agencies are highly exposed to risks associated with outdated or homegrown legacy systems. As subject matter experts for these systems retire, what is being done to plan for the transition of these systems? Are systems being evaluated to determine if they meet current and future business requirements? Are systems and databases secure and capable of preventing data corruption and/or misuse? An ERM approach integrated tightly to a governance structure enables organizations to be more predictive by aligning risk and rewards through the efficient allocation of resources, both strategically and tactically.

Most organizations have tight budgets for IT and therefore, IT spending is rigorously reviewed. A well-structured risk management methodology helps management identify appropriate controls for providing the mission-critical IT capabilities. As IT enables operations, IT risk management processes must be considered more broadly. By evaluating

Today, five themes dominate agencies' risk environments to minimize surprises:

- 1 Changes in the political platform
- 2 Diminishing workforce with loss of subject matter expertise
- 3 Heavier reliance on technology
- 4 Increasing demand on compliance requirements, and
- 5 Increasing taxpayer demand for agency transparency.

All of these themes carry risks with a direct impact on day-to-day business operations. Planning and preparing resources for changes and uncertainty allows an agency to anticipate the risks associated with each of these themes. Asking the right questions at all levels of an agency empowers resources to understand, accept and identify risk associated with day-to-day business operations. Through Enterprise Risk Management, risk analysis turns uncertainty into calculable risk, which is strategically managed.

³ GAO Report GAO-07-310, High Risk Series, An Update.

risks associated with IT, an agency is better armed to secure the IT systems that store, process, or transmit information. They are then able to make informed risk management decisions to justify the expenditures that are part of an IT budget.

4 Compliance and Regulatory Risks

Although many agencies have made significant financial and resource investments to proactively identify risks and meet the demands of compliance, some agencies have yet to realize operational or programmatic improvements. The importance of sound internal controls has been enforced in regulatory standards over the past decades; however, the increased rigor of internal controls, required by regulations such as OMB Circular A-123, has raised the standard for compliance activities to a new level of complexity. In response to a GAO report finding that nearly 41% of \$14 billion in transactions were not properly authorized, OMB deputy director Clay Johnson stated, “We need to do a better job of working with agencies to get them to adhere to policies that exist. On top of that, there are certainly opportunities to strengthen some of these policies and put some of them into law.”⁴

The evolution of internal controls-based compliance requirements continues to grow and is being driven not only by Federal mandates, but also by changes to Sarbanes Oxley compliance requirements within the private sector. Compliance programs require new levels of management, as a shift is occurring from emphasis on controls over financial reporting to all programs within an agency. Unfortunately, agencies are dealing with these challenges by creating silos to handle each requirement as a separate focus area. This creates additional layers of bureaucracy and approvals, resulting in increased costs, decreased efficiency, and frustrated staff. For their efforts to succeed, agencies must efficiently utilize resources and move from reactionary practices to integrated, proactive risk and control management processes. ERMP provides a holistic view of compliance requirements across the agency to reduce duplication of efforts, increase the efficiency of compliance activities, and ensure a standard, manageable response to compliance requirements.

“We need to do a better job of working with agencies to get them to adhere to policies that exist...”

—OMB Deputy Director Clay Johnson

5 Transparency and Accountability Risks

Today, stakeholders and the media are likely to learn about an agency’s unmanaged risk almost instantaneously. As a result, management no longer has time to create response plans to remedy the impact of the occurrence on customers, vendors, and taxpayers before the information is made public. This places a premium on the ability to proactively identify, evaluate, and manage risks. Transparency and accountability risks, often related to reputation risk, are continuing to rise as a major concern within Federal agencies. Taxpayers are demanding more visibility into management processes and associated spending within Federal agencies. To meet the strong demand of increased visibility, the Federal Funding and Accountability Act of 2006 was signed into law on September 13, 2006. This act requires full disclosure of all entities or organizations receiving Federal funds.

To meet the requirements of transparency, agencies are required to spend significant time and energy ensuring a perception of fiscal and operational responsibility within the agency. In order to mitigate the risk of tainting the perception of the agency, leaders must ask: “Are we carefully considering who says what? Does our culture allow and reward the communication of negative information to leadership? If not, do the senior leaders of an agency have accurate and complete information?” Some agencies are addressing these risks and realizing the effort needed to uphold transparency. For example, the National Institutes of Health has established a Director’s Council of Public Representatives in order to educate the public about its mission and operations and solicit their input and participation in the research priority-setting agenda.

⁴ GAO Report GAO-08-333, Governmentwide Purchase Cards.

Mission Drivers for ERM

ERM is implemented for business reasons associated with tactical, operational, and strategic agendas. A tactical approach ensures risks that adversely affect business objectives do not happen or are minimized. An operational approach assesses risks to better manage them. A strategic approach uses risk management to assist in business decision making. Ultimately, ERM should be leveraged within a strategic approach, but can also be very valuable when implemented to address a specific pain point within an agency.

ERM is a proactive and standardized approach to identify, assess, respond, control, monitor, and report risks across an agency to realize value. An ERMP provides an agency with the tools needed to shift risk management focus from issue response and compliance to evaluating risks in business strategy, enhancing decision-making, and improving taxpayer value. Value is created when an agency has a comprehensive, portfolio view of risks and the capability to decipher between a threat and an opportunity through an enhanced decision-making process.

Summary of ERM Benefits

Overall, an ERMP provides an agency with enhanced capabilities to:

- **Manage enterprise-wide risks** – Every agency faces multiple risks that affect different functions and operations. ERM emphasizes the interrelated impact of risks and supports integrated solutions for managing them.
- **Reduce operational surprises and losses** – ERM helps agencies recognize potential adverse events, assess risks and establish responses, thereby reducing surprises and related costs or losses.
- **Improve risk response** – ERM provides tools for identifying and deciding among different risk responses, from acceptance and sharing to reduction or avoidance.
- **Exploit opportunities** – By considering the full range of potential events—rather than just risks—ERM ensures that management can identify and take advantage of positive events quickly and efficiently.
- **Rationalize resources** – ERM creates more robust risk information, which allows management to deploy resources more effectively, thereby reducing overall capital requirements and improving capital allocations.
- **Link growth, risk, and returns** – ERM enhances the capacity to identify events, assess risks, and set risk tolerances consistent with growth and return objectives.

By enhancing these capabilities, an agency is better prepared to carry out and achieve its mission while improving operational performance.

Goals of ERM

Enterprise Risk Management (ERM) programs are implemented to achieve several significant goals, including:

- Engraining risk management as a responsibility throughout all working levels of the agency;
- Breaking down silos to better share risk information across the enterprise;
- Injecting risk analysis into strategic decision making;
- Creating efficiencies in managing risk-related compliance requirements and streamlining internal controls management.

While these goals may not be realized overnight, your agency can begin to monitor and measure progress toward achieving those goals almost immediately. Alignment of individual and unit performance metrics with leading indicators strengthen the control environment and appropriately align investment with risk priority.

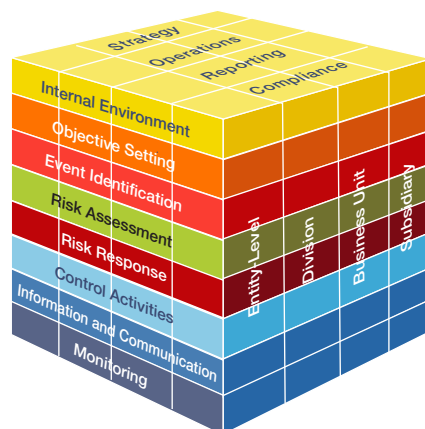
Part 2: PwC's ERM Methodology

Enterprise Risk Management has surfaced as a solution for managing key risks confronting Federal agencies. When an ERM approach is effectively integrated with strategy-setting activities, senior management has a better understanding of how uncertainties impact the overall mission and objectives. The risk profile, displaying the overall risk appetite and risk tolerances across all departments, allows management to “think risk” and build results into strategic planning, capital planning, budget and program management, and performance measurement. An effective ERMP allows organizations to recreate the roles, responsibilities, and relationships of discrete governance, risk, and compliance activities so they act in an integrated, rather than an independent way. This fully integrated approach helps to form an ethical and operational backbone against which an agency can be managed.

PwC brings extensive knowledge and experience delivering of a wide range of services and solutions to Federal risk management. PwC is a Global leader in providing ERM solutions. This depth and experience arms PwC with the tools and experience required to deliver a best fit, tailored ERM program at the agency, department and program level. Our ERM approach provides a comprehensive framework for analyzing each organization's unique risks and developing solutions appropriately tailored to the agency's business environment and culture. The resulting flexibility of our ERM solution enables the methodology to be adopted as a common platform across the agency to face the challenges associated with governance and control, operational oversight, or strategic planning drivers.

Implementing a Proven Approach

Enterprise Risk Management Programs are based upon a working knowledge of an enterprise's internal control environment and risk management structure. PwC's methodology leverages the Committee of Sponsoring Organization (COSO) “COSO 2”, ERM integrated framework, co-authored by PwC and recognized as a leading framework within both the private and public sector for risk and control management. The COSO Framework is recommended by the SEC as an accepted internal control framework to guide corporate compliance with Sarbanes Oxley. COSO requires an entity-level activity- or process-level internal control focus and an activity- or process-level focus with three objectives: effectiveness and efficiency of operations, reliability of reporting, and compliance with applicable laws and regulations.



1. **Understand** the agency's goals as well as the internal environment defined by policies, structure, ethical values, and philosophy.
2. **Plan** an assessment process that supports the agency's goals and balances risk management benefits and investments. Identify risks that may impact the agency's operations and goals.
3. **Assess** readily identifiable significant risks. Determine impact, probability, and immediacy of risks. Prioritize risks based on defined criteria.
4. **Evaluate and Report** risk status. Identify gaps in compliance policies, taking into consideration the controls and safeguards already in place.
5. **Define Corrective Actions** to respond to the risks and maintain compliance with risk management policies.
6. **Monitor** progress of corrective actions. Continue to identify new risks.

WP ERM-002

Figure 1: Integrated Risk Assessment Methodology.

Elements of our methodology are illustrated by the “COSO cube” in **Figure 1** on the previous page. These elements provide the foundation of an effective ERMP implementation: the internal environment; objective setting; event identification; risk assessment; risk response; control activities; information and communication; and monitoring.

Every Federal agency has a different risk maturity level and a different approach to managing risk and control processes. PwC understands the need to deliver a tailored ERM program for each customer that leverages current risk management processes. Utilizing the COSO framework as a foundation of Enterprise Risk Management provides a comprehensive framework for analyzing each agency’s unique issues and developing solutions appropriately tailored to the agency’s business environment and culture.

Managing Risk to Attain Objectives

Leveraging the COSO framework, PwC develops a tailored ERM approach for each agency. Each tailored ERM Program provides the foundation for a transformation effort across various lines of business. It targets the improvement of management controls, the reduction and management of risks, and the improvement of operations.

The PwC approach follows a six-step implementation approach: understand, plan, assess, evaluate and report, define corrective actions, and monitor. Each phase within the PwC ERM methodology is summarized below:

- **Understand** – PwC assesses an agency’s risk and control environment using a Risk Management Maturity Model (RMMM) consisting of five levels of risk “maturity” (**Figure 2**). An agency is evaluated across people, process, and technology competencies using interviews with key stakeholders. This process provides a view of an agency’s overall risk universe by identifying sources of risk within a baseline risk library and promoting an understanding of how risk is managed in the agency today.

Assessing and creating a Risk Management Maturity Model allows the agency to determine whether existing risk processes are adequate, identify realistic targets for improvement, and produce action plans for developing or enhancing a risk management maturity level.

Level 1 Ad Hoc	Level 2 Managed	Level 3 Standardized	Level 4 Integrated	Level 5 Optimized
Risk management is not well understood by management or staff and is seen as an unnecessary expense. Without any defined risk management policies or procedures, individuals only have time to worry about “getting it done.”	Knowledge of risk management exists but is driven by external reporting/compliance requirements. Policies and procedures are established for individual business units, not organization-wide. However, the individual business units lack the ability to apply risk management procedures consistently and continuously.	The organization has established an explicit risk culture and routinely incorporates risk management in programs, applying risks and lessons learned from previous, similar programs. Risk management procedures are standardized in an enterprise risk framework that is available to all employees.	Uniform processes are used to manage risk throughout the organization. Business unit and organization-wide risks are measured and linked across the enterprise. An integrated dashboard monitors risk management categories. Understanding of the organization’s risk profile helps drive strategic decision making.	Risk management is embedded in how the organization does business, and standardized tools are in place to fully support goals. Risk information is continuously developed and actively used to improve all organization processes.

Figure 2: Excerpt of Risk Management Maturity Model (RMMM) .

The primary value of the maturity model approach is that it gives risk managers, leadership, and customers a common framework to address issues and set priorities, so that the organization has a clear direction toward improving risk and control management. This approach enables organizations to efficiently build their Enterprise Risk Management capabilities and ultimately drive towards higher maturity levels.

At higher maturity levels, risk associated with operational processes is typically lower, while the degree of control, predictability, effectiveness, and efficiency is higher. PwC assesses and benchmarks the risk and control maturity score to provide an agency with quantifiable measures to determine the success of an ERMP. Additionally, the benchmark maturity scores provide visibility into how each organization within an agency is driving towards higher risk and control maturity levels. Monitoring and reporting this maturity provides visibility on the future sustainability of risk management effectiveness. The underlying assumption is that the more mature your risk management processes are, the greater sustainability you will experience in effectively managing risks. Increasing risk and control management maturity leads to operational efficiencies and increased customer satisfaction.

- Plan** – Once an agency understands its risk environment, it is better prepared to evaluate the events impacting the meeting of strategic objectives and the actions needed to mitigate the risks associated with each potential event. An agency can then better develop and communicate a consistent message on how it will work to mitigate these risks. PwC works with each agency to establish a detailed ERM implementation plan and roadmap to meet ERM objectives. This roadmap encompasses the following steps: align risks to strategic objectives and priorities; enable risk assessments; introduce consistency to methods for managing risk across the agency; integrate control activities; and improve risk communication, monitoring, and reporting. The implementation plan outlines the critical tasks, activities, and personnel required for an agency to implement ERM. Highlighted within this plan are the tasks associated with end-to-end process mapping, risk and control identification, and assessment and compliance integration.
- Assess** – In order to capture all risks and controls within an agency, critical processes are documented, and an associated objective is established. Each process is evaluated to determine operational risks impacting the meeting of the defined objective. Associated controls and control gaps are identified. To capture complete risk information, each process is linked to its appropriate compliance requirements. Any risks associated with meeting the compliance program are documented.
- Evaluate and Report** – To efficiently and effectively share risk information throughout the agency, PwC works with Federal agencies to leverage the existing vertical organizational structure (e.g., the FMFIA Assessable Unit (AU) structure) in parallel to developing “Core Areas,” or like functions, that align processes horizontally across the organization, regardless of geographic location. With this information, an agency is able to compare like processes and share risk information both vertically and horizontally across the agency. It enables the agency to reflect a collective intelligence with regard to risks, controls, and governance. For example, an Information Technology or Data Storage Core Area may be created that includes all processes associated with the storing of sensitive information. An agency is then able to look across the enterprise and share risk and control information to mitigate similar risks associated with loss of sensitive information to prevent issues from arising.
- Define Corrective Actions** – PwC works with Federal agencies to establish a uniform process across the agency that encourages self-identified reporting and captures ‘incidents’ or deficiencies within processes that could keep an agency from achieving its objectives. PwC leverages remediation procedures included in corrective action plans (CAPs) and Plan of Actions and Milestones (POAM) to provide a standardized



Figure 3: ORCA Framework.

PwC uses its Objectives, Risks, Controls, and Alignment (ORCA) Framework, depicted in Figure 3, to evaluate business objectives, the related risks to achieving those objectives, and management’s method to manage those risks. Identifying and assessing risk and control within an ERMP provides a standard structure and definition for any internal assessments required to address the full scope of the processes within an agency.

process across the agency to identify risks, risk owners, and to resolve control gaps within an agreed timeframe. CAPs and POAMs include a framework that establishes a detailed step-by-step guide to resolving control gaps and incidents.

If an agency identifies the loss of sensitive information as a risk, they are able to evaluate the controls currently mitigating the risk and are able to better identify a control deficiency or gap. An agency can then elevate the risk and assign an individual or team accountable to define the corrective actions needed and resolve the control gap.

- Monitor** – Through the use of an integrated dashboard, PwC establishes a monitoring and reporting framework that establishes accountability throughout an agency. An ERM dashboard has the capability to summarize and graphically report risk information across an agency and is used as a decision making tool. An ERM Dashboard is leveraged throughout the agency from the executives down to process owners. It allows for ongoing risk monitoring and reviewing of the status of risks control information (Figure 4).

Armed with an understanding of the risk management maturity level and risk environment, a plan clearly defining the scope and goals of an ERMP can be developed to include the establishment of a risk management governance structure to carry out the ERMP. After the plan has been established, the higher priority risk categories are further evaluated within the “assessment” phase to determine if risk management practices are sufficient to mitigate to the acceptable level of risk. This risk information is then reported to multiple levels of the agency through the established governance structure. If weaknesses were identified while assessing agency risks, corrective actions are defined. Additional actions are performed as needed, such as improving or adding controls to prevent the risks from becoming issues.

Through this tailored implementation approach, an agency is positioned to meet its objectives and realize its ERMP vision. ERMP then becomes an integrated and embedded element of agency operations, culture and ethical environment. ERM is institutionalized across the enterprise, aligned with individual and management responsibilities forms the basis for measuring performance and individual accountability within an agency.

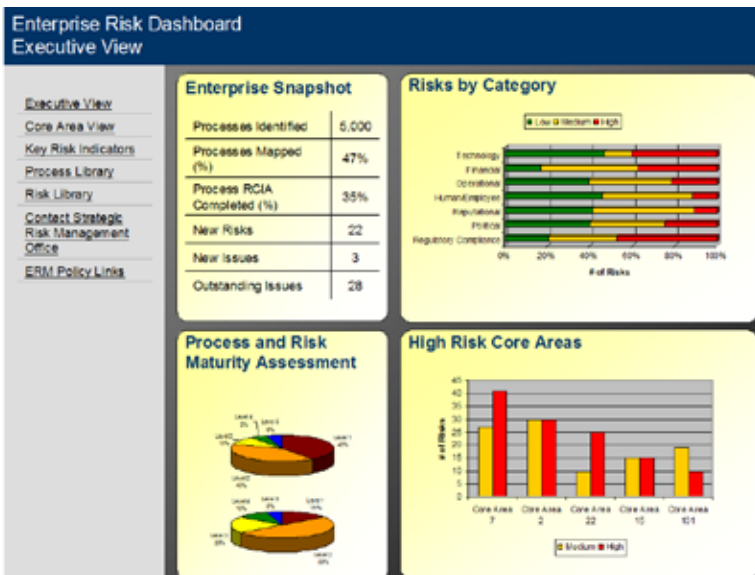


Figure 4: Enterprise Risk Dashboard.

Part 3: Achieving ERM Benefits

Infrastructure is critical to the success of an ERM program. Establishing lines of authority and identifying parties responsible for oversight, management, and execution is a necessary first step to implementing ERM. In the past, risk management, organizational governance, and compliance have generally been viewed as discrete areas of focus, managed as separate functions across an agency. However, this approach often results in accountability and communication gaps as well as confusion. Organizations should re-think the roles, responsibilities, and relationships of discrete governance, risk, and compliance activities so they act in a united, rather than an independent way. This fully integrated approach, shown in **Figure 5**, helps to form an ethical and operational backbone against which an agency can be managed.

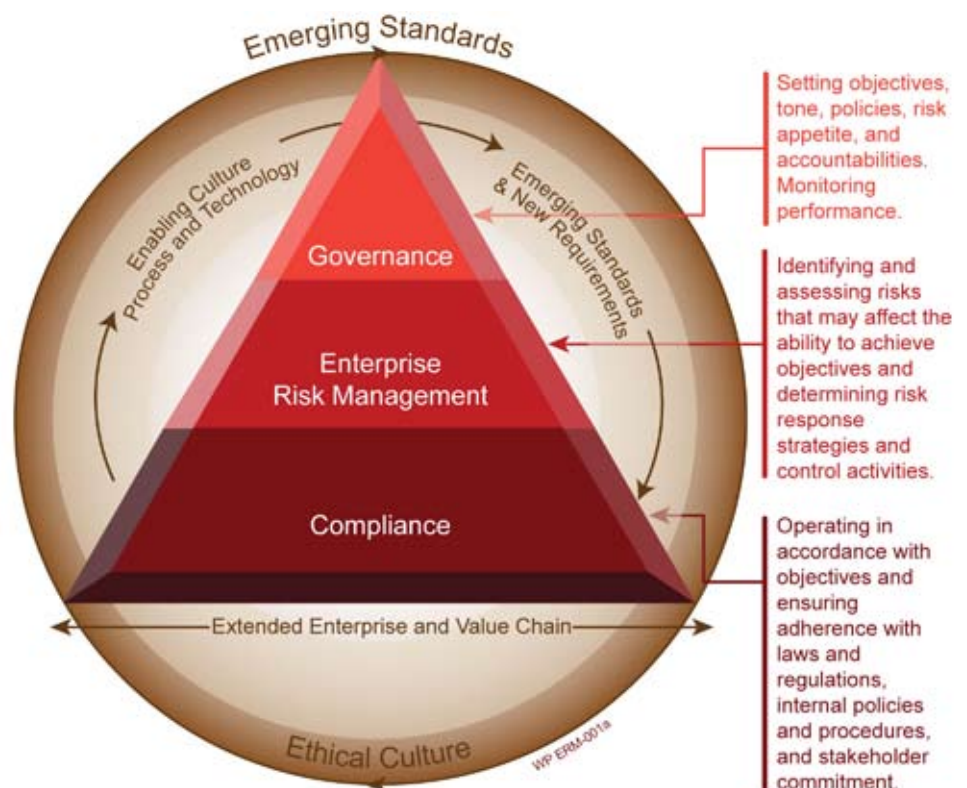


Figure 5: Governance, Risk, and Compliance Model.

Raise Agency Awareness

The identification and assessment of risk at an enterprise level requires a shift for the executive, the manager, and the employee in the agency. Agencies must modify existing risk and control practices to ensure that enterprise risks are managed as a distinct activity throughout the agency. Communication is the cornerstone of change management. An informed, well-trained workforce is one of the key maturity markers for a robust risk management environment. Raising agency awareness of ERM should entail:

- Establishing agency-wide commitment to the program to reinforce achievement of strategic objectives
- Providing information that addresses the major aspects of the changes: what is happening; when will the changes be implemented; how the changes affect daily operations; and who has responsibility for the changes
- Communicating the program benefits and objectives through an internal promotional campaign

ERM helps organizations emphasize key risks in strategic and business decisions, distinguishing risks as opportunities versus threats. Executives are armed with a comprehensive portfolio view of organization risks and apply their understanding in the decision-making process.

An enterprise view of risks also opens the dialogue between silos to create continuity between similar business processes. Unencumbered access to risk and control information is the focus of ERM. PwC incorporates standardized risk monitoring and reporting tools to ensure communication, coordination, and collaboration of risk and control information across the agency. Identification and mitigation of risks are now viewed from an enterprise perspective, not based on individual business processes.

ERM Goal Setting: Establishing a Framework for Measuring Success

In discussing performance management around ERM, it is important to understand two distinct types of performance measures: output-oriented measures and outcome-oriented measures. Both types of performance measures can play an important role in how to measure success in an ERM program. Output measures provide incremental feedback to leadership on how an ERM program is progressing, and are often easily quantifiable. Outcome measures are result-oriented and are tied more directly to achieving the agency's overarching goals and success of the ERMP. Establishing output and outcome measures helps set short- and long-range goals for an Enterprise Risk Management Program.

Establishing a framework for organizations to assess current risk management capabilities and identify priority areas and initiatives for development is also important. This can be achieved through the PwC ERM Maturity Model. The PwC ERM Maturity Model approach aims at measuring an organization's risk management maturity relative to best practices, industry benchmark data, and the perceived risk tolerance of the organization. It considers such elements as: leadership view of risk; corporate view of risk; communication of risk; Human Resource risk; finance risk; technical risk; operational/project risk; and business continuity planning.

Integrating Existing Initiatives: Smart Moves to Cut Cost, Effort, and Disruption

Enterprise Risk Management provides a framework for integrating shared activities into a single, cohesive program, leveraging existing structures and resources to build a single, cohesive program meeting the objectives of existing initiatives while providing an enterprise-wide, predictive platform for decision making.

Tools, processes, roles, and responsibilities inherent in an ERM program naturally support other enterprise initiatives, such as process improvement, business activity monitoring, and performance management. Perhaps most significantly from a resource allocation perspective, ERM also supports the integration of existing compliance programs in Federal agencies.

PwC Principles

Start with what you have: Simple, but realistic. A successful ERM implementation will integrate with the existing structural elements within the Federal agency that were perhaps built with a different program perspective, but still reflect the tenets of ERM.

Understand that the whole is made up of the parts: The contribution and risk exposure provided by each organization within the agency to the agency mission is based on what activities or functions the organizations performs or oversees in alignment with the agency mission. Many compliance and oversight activities are focused on the process level, and by taking a bottom-up approach, return on resource investment is maximized through dual-purposing activities from the start of implementation.

Build existing programs into the Enterprise Risk Management Process: When integrating ERM into existing or ongoing activities, it is imperative to establish enterprise-wide presence. For each element proposed for the program or as an integrated element, evaluate its contribution to the enterprise perspective in the context of the sponsoring initiative and/or program.

The activities common to ongoing compliance programs are often targeted to different organizational units within an agency. The commonality in the themes related to risk, controls, and mitigation and remediation activities are lost as each organization pursues its individual compliance objectives. Without coordination of risk and control activities, risk and compliance management efforts are fragmented.

In the planning and integration of ERM within a Federal agency, PwC has three basic principles for maximizing the impact while minimizing the cost of an enterprise risk management program.

1 Start with what you have: Building a workable infrastructure

Successful implementation of ERM in an existing agency requires a careful inventory of the infrastructure and reporting structures already defined in the organization. At least two elements of an ERM infrastructure will exist within the current infrastructure of an agency – the executive council, senior assessment team, or other oversight function that will maintain the enterprise perspective of the implementation and empower its success; and the lowest level of accountability within the organization. For example, with its Managers' Internal Control (MIC) Program, the Department of Defense has defined an "assessable unit" as the lowest level of accountability. The strong vertical chains of command can be successfully integrated into the infrastructure of ERM as the foundational ERM working group, chartered to represent the interests of the organizational units, even as cross-cutting horizontal perspectives are introduced for the enterprise-wide representation.

2 The whole is made up of its parts: Bottoms up, enterprise process management

Addressing the question, "What are the risks to my agency's mission?" and "How do I monitor and predict them?" can be answered, in part, by managers and employees in the aggregation of their responses to the questions "What do you do?" "Where are your risks?" By integrating existing programs and initiatives for evaluation of internal controls, the resources devoted to documenting processes within the agency or performing assessments can be dual-purposed. When protocol is standardized and data storage is centralized for ERM, documented processes can be used within an ERMP, but also leveraged for use within training programs, knowledge transfer, and compliance programs. Further integration of the ERM cycle with the compliance and reporting cycles will limit the disruption to ongoing mission-centric work for risk management.

3 Build existing programs into the ERM process: Integrate performance management and compliance activities

The President's Management Agenda focuses on five initiatives to improve government management. The focus of these initiatives is "to address the most apparent deficiencies where the opportunity to improve performance is the greatest." By leveraging an ERMP within performance management, agencies are more prepared to identify opportunities to respond to performance deficiencies by adding the "what if" dimension? That is, what could happen to hinder the achievement of an objective?

Organizations can employ risk management to account for the "what if" dimension in strategic planning. By associating risks with Balanced Scorecard metrics, for example, an agency can add predictive ability to its reporting system. The Balanced Scorecard already details what the organization wants to achieve. ERM provides input into the likelihood of achieving the objectives and enables the proactive identification of steps to mitigate the potential risks.

In addition to the increased emphasis on performance management, compliance management continues to increase in complexity. In response to the increased regulatory attention and direction for the appropriate controls for the resources entrusted to the

Federal manager, there are numerous compliance programs in place, with resources devoted to documenting and assessing the effectiveness of the oversight and control programs in place. The Federal Financial Managers Integrity Act (FMFIA), and related implementation guidance has required significant time and resources dedicated to initiating and maintaining programs managed at the agency level, with implications at the Department level.

Risk and compliance management has often been fragmented throughout organizational silos, resulting in a duplication of technologies and efforts with inconsistent approaches, measurement, and reporting. The lack of central visibility and oversight has resulted in islands of information trapped in documents and individuals throughout the enterprise. As **Figure 6** illustrates, common activities associated with numerous compliance programs are repeated and occur with little coordination.

As mentioned above, the scope of compliance programs address specific risk management activities; however, ERMP is structured to encompass all risks impeding an agency from meeting its goals and objectives, which includes compliance-related objectives. ERMP provides the foundation to manage all risks and controls information across an agency. This foundation supports a centralized approach to compliance management, including the following characteristics:

- Central management oversees all efforts (i.e., programmatic, financial, and institutional);
- Guidance originates from a single source;
- Efforts are allocated and assigned by work stream; and
- Corrective Action Plans (CAPs) are integrated across work streams.

Whether in preparation for reorganization, data standardization, audit support or compliance activities, each agency has devoted precious resources to developing parts and pieces of an overall enterprise risk understanding. Many agencies, however, remain ill-equipped to predict or proactively address emergent risks to the mission and strategic risks of the agency, due to fragmentation of compliance efforts. Enterprise Risk Management can provide the framework for maximizing the resource investment, minimizing compliance costs, and providing a true enterprise-wide, predictive solution.

Increasing Internal Visibility and External Transparency: The Role of Technology

To gauge performance information in a timely manner, best business practices show that agencies should leverage technology that enables them to monitor performance information on a continuous basis. Agencies that have adopted these practices use web-based software that collects Key Performance Indicators and Key Risk Indicators from operational systems, which allow for drill-down, root cause analysis. Such technology helps agencies improve performance and develop strategies that more accurately reflect changing business conditions.

Advancing an organization’s enterprise risk management capabilities depends on the integration of people, processes, and technology. The effectiveness of any ERM technology also depends on critical success factors in each of these three areas. On the other hand, neglecting competencies in any of these three areas jeopardizes the value of a dashboard implementation. For example, an organization could deploy a system with state-of-the-

	ERMP	FMFIA	FFMIA	A-123 (A)	IPIA	FISMA	FIAR
Process flowcharts	•	•		•			•
Identify process risks	•	•	•	•	•	•	•
Risk Assessments	•	•	•	•	•	•	•
Identify controls	•	•	•	•	•	•	•
Evaluate controls	•	•	•		•		•
Report on controls	•	•	•	•	•	•	•
Corrective Action Plans (CAPs)	•	•		•	•	•	•
Prioritize controls	•			•	•		

Figure 6: Common Compliance Activities.

art technology, but its implementation would fail if the resources are not available to support its day-to-day management and oversight.

The marketplace for technology that supports ERM is extensive and quite diverse. PwC's approach is to work with your organization to identify a best fit and best value technology to support your ERM program. Depending on your organization's requirements, PwC can tailor a technical approach to meet any combination of typical ERM system features such as: real-time visual reporting, data repositories, workflow, performance management, and analytics. Types of technical solutions supporting ERM can include the following:

- **Dashboards** – Dashboards foster enhanced aggregation and visibility of important ERM information across an organization. An important aspect of our ERM implementation approach is to identify key performance metrics and important ERM knowledge to share dynamically within an ERM dashboard.
- **Document and Knowledge Management** – One of the key tenets of ERM is knocking down departmental silos to make risk-related information more accessible across the organization. Document and knowledge management solutions facilitate the management and dissemination of key program information. ERM policies and procedures complement existing document and knowledge management tools to further support your organization's ERM program.

- **Business Activity Monitoring (BAM)** – Business Activity Monitoring (BAM) provides real-time information about the status and results of various operations, processes, and transactions so business decisions can be informed, can quickly address problem areas, and can re-position organizations to take full advantage of emerging opportunities.
- **Governance, Risk, and Compliance Systems (GRC)** – PwC has worked extensively with leading industry technology leaders, such as SAP and Oracle, around forming and implementing enterprise GRC solutions. PwC currently has the largest trained SAP GRC Access Controls (Virsa) resource pool in the world, with over 50 successful implementations.

Performance measurement is no longer used as a mere yardstick to gauge numbers and ratios but, rather, as a catalyst for improvement and change. Though performance measures themselves cannot alter an agency's culture, they can be a powerful lever for reinforcing organizational strategy by revealing baseline values, establishing accountability, and making organizational goals visible. Technology can be a key enabler in collecting, sharing, and reporting information to measure the success of your Enterprise Risk Management initiatives.

Part 4: Summary

The PwC ERM solution is designed to improve performance through the efficiency and effectiveness of risk management, while enhancing its organizational visibility supporting a robust decision-making environment. The PwC ERM solution:

Links risks and opportunities to organizational goals and objectives

Enhances the capacity to identify events, assess risks, and set risk tolerances consistent with organizational goals and objectives.

Exploits opportunities and mitigates risks

Assists management to identify and take advantage of positive events quickly and efficiently, as well as, mitigate risks that impede strategic goals and objectives.

Bridges organizational silos

Creates continuity between similar business processes and across the organization by opening lines of risk communication, coordination, and collaboration to effectively and efficiently identify and mitigate risks.

Reduces operational surprises and losses

Creates a framework to recognize potential adverse events, assess risks, and establish responses, thereby reducing surprises and related costs or losses.

Meets complex Federal compliance requirements

Acts as a central conduit for management of enterprise-wide risk information to meet numerous compliance requirements and allow employees to work smarter by eliminating multiple data calls.

A strategic and proactive approach to risk management contributes not only to an efficient and effective fulfillment of compliance requirements, but also enables agencies to realize additional benefits. Agencies are enabled to respond earlier, more flexibly, and more comprehensively to change.

This not only enhances their public image, but also supports the justification for Federal funding, by demonstrating a firm foundation for the long-term strategic plan of the agency.

ERM helps organizations emphasize key risks in strategic and business decisions, distinguishing risks as opportunities versus threats. Executives are armed with a comprehensive portfolio or enterprise view of organizational risks and can apply understanding in the decision-making process.

An enterprise view of risks also opens the dialogue between traditional organization silos to create continuity between similar business processes. Through an ERMP, agencies are armed with a proactive and standardized approach to identify, assess, respond, control, monitor, and report all risks across an agency to realize value. Value is ultimately created when agency leadership has a comprehensive, portfolio view of risks and the capability to decipher between a threat and an opportunity through an enhanced decision-making process. ERM breaks down the traditional silos where specific risk management activities are housed and elevates those key risks impacting the organization's critical mission and objectives. In return, an agency is able to strengthen mission focus and maximize the return on taxpayer dollars. A fully integrated ERM approach helps to form an ethical and operational backbone against which an organization can be managed.

The key results of an ERM implementation include the following: reliable risk management information delivered to managers' desktops, with drill-down capabilities supporting fact-based decision making; a process to ensure on-going data integrity; and a standardized, integrated risk management process in line with organizational accountabilities to drive strategy and action. PricewaterhouseCoopers is well placed to provide leading edge risk and regulatory advisory services. We have invested significantly in enterprise risk management (ERM) thought leadership through the publication of the COSO ERM framework and our Integrated Governance, Risk and Compliance (iGRC) framework. To turn our thought leadership into action, we have developed robust methodologies that promote consistency and quality engagement delivery. We have established a proven track record of providing value-added solutions to our clients.

Contact information:

Melissa Glynn
Principal
melissa.glynn@us.pwc.com
703.918.1268

Robert Speer
Managing Director
robert.speer@us.pwc.com
(703) 918-1041

Joseph Kull
Director
joseph.kull@us.pwc.com
(703) 918-1320

