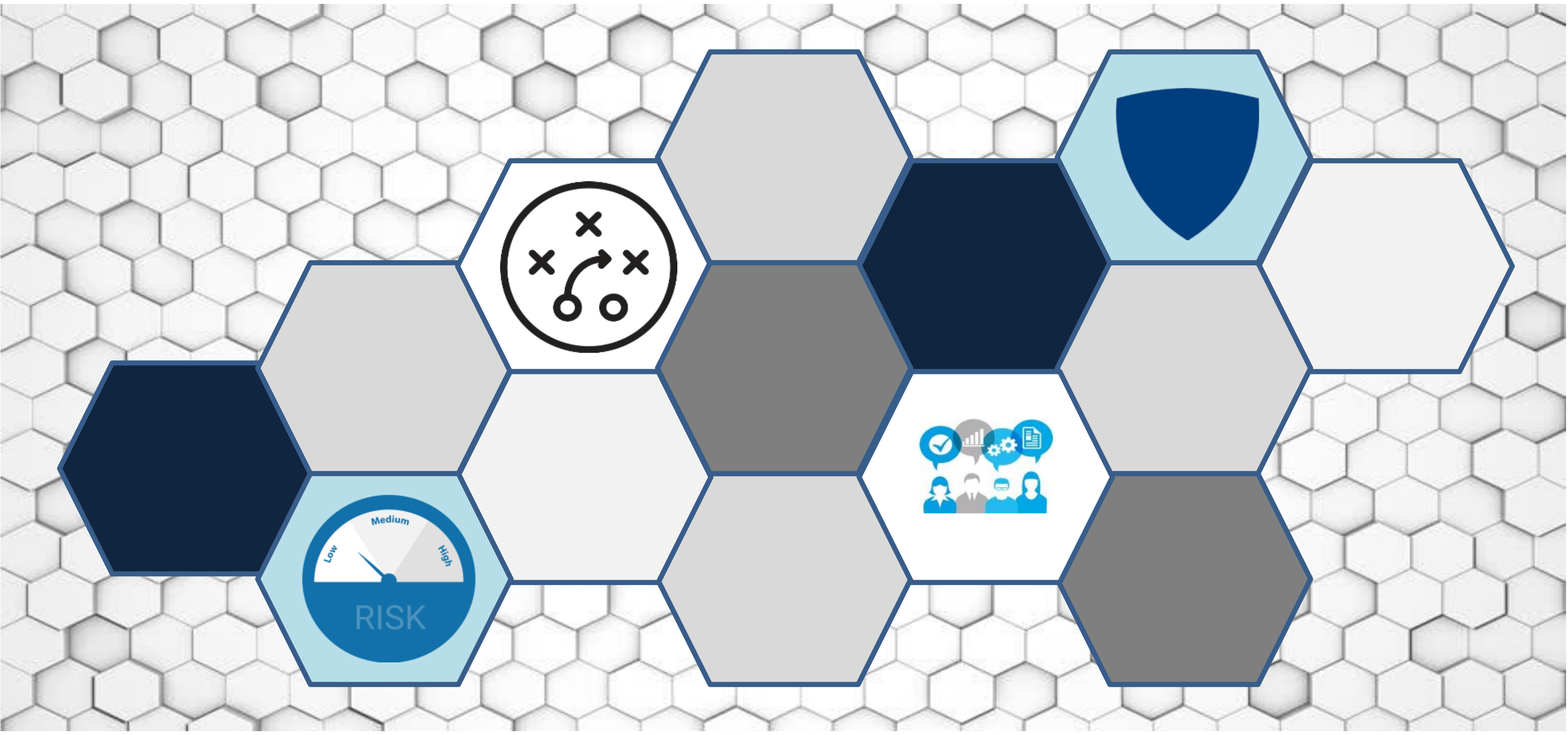
Playbook:

Enterprise Risk Management for the U.S. Federal Government



Developed and issued in collaboration with Federal Government organizations to provide guidance and support for ERM.

CFO
UNITED STATES
CHIEF FINANCIAL
OFFICERS COUNCIL

PIC.gov
Performance Improvement Council

CFO
UNITED STATES
CHIEF FINANCIAL
OFFICERS COUNCIL

PIC.gov
Performance Improvement Council

MEMORANDUM FROM Chief Financial Officers Council (CFOC)
Performance Improvement Council (PIC)

DATE: July 29, 2016

SUBJECT: Playbook: Enterprise Risk Management for the U.S. Federal Government

The Chief Financial Officers Council (CFOC) and the Performance Improvement Council (PIC) release the *Playbook: Enterprise Risk Management (ERM) for the U.S. Federal Government* (Playbook). The Playbook guidance and accompanying appendices are tools designed to help government departments and agencies meet the requirements of the revised Office of Management and Budget Circular A-123. They are also designed to provide high-level key concepts for consideration when establishing a comprehensive and effective ERM program. The Playbook specifically addresses the additional requirements included in Section II in A-123, which defines management's responsibilities related to ERM, to help departments and agencies make better decisions based on a more holistic view of risks and their interdependencies.

The Playbook is the result of an interagency effort convened by the Office of Executive Councils and included risk practitioners and cross function representation from more than twenty federal agencies to gather, define, and illustrate practices in applying ERM in the Federal context. The final document and subsequent versions will be posted to the CFOC and PIC websites.

To help affected agencies implement A-123, the Playbook will be updated with information and examples as programs' and agencies' ERM capabilities mature. Additionally, forums to discuss issues that arise and share best practices related to ERM across the Federal Government will be convened. As part of these on-going efforts, we will continue to accept any comments, suggestions, and examples for the Playbook at support@cfo.gov.

cc: Dave Mader, Controller of the United States of America
Mark Reger, Deputy Controller of the United States of America
Lisa Danzig, Federal Chief Performance Officer, OMB
Dustin Brown, Deputy Associate Director for Performance and Personnel Management, OMB

Table of Contents

I. Introduction

***Playbook: Enterprise Risk Management (ERM) for the U.S. Federal Government* ("Playbook") is the result of an interagency effort to gather, define, and illustrate practices in applying ERM in the Federal context.** This Playbook and accompanying appendices are tools designed to help government departments and agencies meet the requirements of the revised OMB Circular No. A-123. They are also designed to provide high-level key concepts for consideration when establishing a comprehensive and effective ERM program. Nothing in this Playbook should be considered prescriptive. All examples provided should be modified to fit the circumstances, conditions, and structure of each agency (or other government organization). The goal of the Playbook is to promote a common understanding of ERM practices in agencies to support effective and efficient mission delivery and decision making processes, such as policy and program development and implementation, program performance reviews, strategic and tactical planning, human capital planning, capital investment planning, and budget formulation. The Playbook is intended as a useful tool for management. It is not intended to set the standard for audit or other compliance reviews.

The material in this document is intended to be:

1. Useful to employees at all levels of an agency;
2. A useful statement of principles for senior staff, whose leadership is vital to a successful risk management culture and ERM program implementation;
3. Practical support for operational level staff who manage day-to-day risks in the delivery of the organization's objectives;
4. A reference for those who review risk management practices, such as those serving on Risk Committees; and
5. Helpful for implementing the requirements of OMB Circular No. A-123, ERM Section II[1].

To manage risk effectively, it is important to build strong communication flows and data reporting so employees at all levels in the organization have the information necessary to evaluate and act on risks and opportunities, to share recommendations on ways to improve performance while remaining within acceptable risk thresholds, and to seek input and assistance from across the enterprise.

A. Using This Playbook

This Playbook is intended to assist Federal managers by identifying the objectives of a strong ERM process, suggesting questions agencies should consider in establishing or reviewing their approaches to ERM, and offering examples of best practices.

An agency-wide ERM program should enhance the decision-making processes involved in agency planning including strategic and tactical planning, human capital planning, capital investment planning, program management, and budget formulation. It should build on the individual agency's risk management activities already underway and encompass all of the agency's operations.

[1] Note that OMB Circular A-123 does not seek to describe a comprehensive ERM program.

Responsibility for managing risks is shared throughout the agency from the highest levels of executive leadership to the service delivery staff executing Federal programs. Effective risk management, and especially effective ERM, is everyone's responsibility.

This Playbook was written by a group of agency risk practitioners and is not an authoritative part of OMB Circular No. A-123 or other guidance. While this Playbook provides the foundation for applying ERM principles and meeting the requirements of A-123, it is not an exhaustive manual with specific checklists for implementing ERM. Each agency should determine what tools and techniques work best in its unique context. ERM is an iterative process. As agencies' ERM capabilities mature, their implementation of the recommendations in this Playbook should be modified to fit the circumstances, conditions, and structure of each entity. This Playbook is intended to provide guidance to help managers make better-informed decisions based on a more holistic view of risks and their interdependencies. It is not intended to set standards for audit or other compliance reviews.

The appendices include examples of documents that some agencies have found helpful. Again, they are not intended to be prescriptive.

B. What is Risk Management? What is ERM? Why Do Government Agencies Need Them?

Risk is unavoidable in carrying out an organization's objectives. Government departments and agencies exist to deliver services that are in the public interest, especially in areas where the private sector is either unable or unwilling to do so. This work is surrounded by uncertainty, which both poses threats to success and offers opportunity for increasing value to the American people.

While agencies cannot respond to all risks, one of the most salient lessons from past crises and negative reputational incidents is that both public and private sector organizations would benefit from establishing or reviewing and strengthening their risk management practices. Agencies are well advised to work to the greatest extent possible to identify, evaluate, and manage challenges related to mission delivery and manage risk to a tolerable level.

For the purposes of ERM, **Risk** is the effect of uncertainty on objectives. **Risk management** is a coordinated activity to direct and control challenges or threats to achieving an organization's goals and objectives. **Enterprise Risk Management** is an effective agency-wide approach to addressing the full spectrum of the organization's significant risks by considering the combined array of risks as an interrelated portfolio, rather than addressing risks only within silos. ERM provides an enterprise-wide, strategically-aligned portfolio view of organizational challenges that provides improved insight about how to more effectively prioritize and manage risks to mission delivery[2].

Effective ERM facilitates improved decision making through a structured understanding of opportunities and threats. Effective ERM also helps agencies implement strategies to ensure effective use of resources, enable an optimized approach to the identification and remediation of compliance issues, and promote reliable reporting and monitoring across business units. It helps drive a culture of better understanding,

[2] The Office of Management and Budget *Circular A-11, Preparation, Submission, and Execution of the Budget, Section 270.24.*

disclosure, and remediation of agency risks. ERM also helps agencies strengthen their ability to evaluate alternatives, set priorities, and develop approaches to achieving strategic objectives. The adoption of consistent risk management processes and tools can help to ensure that risks are managed effectively, efficiently, and coherently across an agency.

An ERM framework allows Federal agencies to increase risk awareness and transparency, improve risk management strategies, and align risks to each agency's risk appetite and risk thresholds. **Risk Appetite**[3] is the articulation of the amount of risk (on a broad, macro level) an organization is willing to accept in pursuit of strategic objectives and the value to the enterprise. **Risk Tolerance**[4] is the acceptable level of variance in performance relative to the achievement of objectives. It is generally established at the program, objective, or component level. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite. Federal agencies will be most successful in managing risks when there is a high level of awareness and ownership of risk management at all levels of the agency.

C. Integrating ERM into Government Management Practices

Successful integration of ERM into agencies' day to day decision-making and management practices enables agencies to leverage opportunities and avoid, mitigate, and transfer risk, resulting in more resilient, effective, and efficient programs. ERM can help to focus and inform decisions, by defining goals and objectives, advocating for and aligning resources, monitoring progress, and ensuring compliance with applicable laws, regulations, and controls.

Recent OMB guidance calls for the integration of ERM into existing Government management practices. As shown in Figure 1, this means that risks across the enterprise be considered and prioritized as part of CXO/operations support, program management, budget decisions, and strategic planning. The importance of integrating ERM into existing government management practices was also highlighted in the President's 2017 Budget:

ERM Pitfall

ERM not integrated

ERM should not be an isolated exercise, but instead, should be integrated into the management of the organization and eventuallv into its culture.

> *Enterprise Risk Management:*
> *These practices provide the framework to shape future initiatives in Federal performance management. As work continues on agency internal controls and enterprise risk management, 2017 offers an opportunity to integrate risk management profiles around mission and mission support functions in agency strategic planning and reviews. Opportunities also exist for collaboration and integration across evidence, evaluation, and performance teams.*

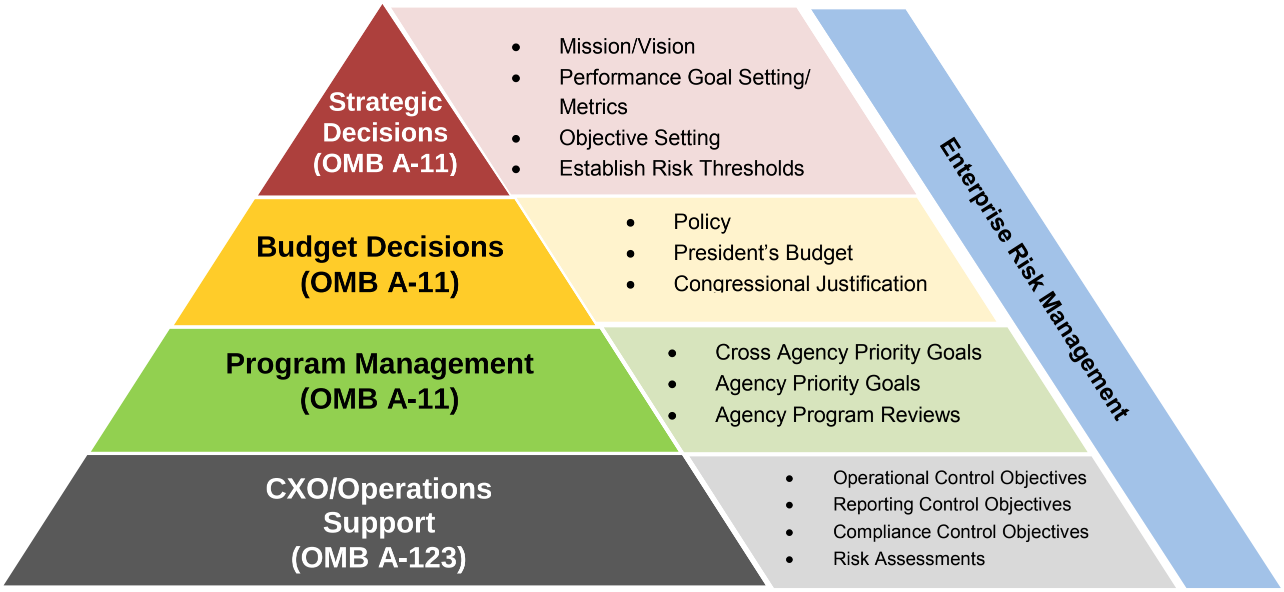
Section II of OMB Circular No. A-123 defines management's responsibilities for ERM and includes requirements for identifying and managing risks. It encourages agencies to establish a governance structure, including a Risk Management Council or Committee (RMC) or similar body; requires the

[3] The Committee of Sponsoring Organization of the Treadway Commission (COSO) *Enterprise Risk Management-Integrated Framework, p. 20*

[4] Ibid.

development of “Risk Profiles” to identify major risks arising from mission and mission-support operations; and analyze those risks in relation to achievement of strategic objectives. It complements Section 270 of OMB Circular No. A-11 that discusses agency responsibilities for identifying and managing strategic and programmatic risk as part of agency strategic planning, performance management, and performance reporting practices. Together, these two Circulars constitute the core of the ERM policy framework for the Federal Government with specific ERM activities integrated and operationalized by Federal agencies. The following figure shows the interplay among OMB Circulars A-123 and A-11 and controls, program management, budget, and strategic decisions within the ERM framework.

Figure 1: The ERM Policy Framework


Strategic Decisions (OMB A-11)
Mission/Vision
Performance Goal Setting/ Metrics
Objective Setting
Establish Risk Thresholds
Budget Decisions (OMB A-11)
Policy
President’s Budget
Congressional Justification
Program Management (OMB A-11)
Cross Agency Priority Goals
Agency Priority Goals
Agency Program Reviews
CXO/Operations Support (OMB A-123)
Operational Control Objectives
Reporting Control Objectives
Compliance Control Objectives
Risk Assessments
Enterprise Risk Management

As shown in Figure 1, an effective ERM program is an integral part of the agency’s strategic decision making process. Agencies should establish risk thresholds and identify top risks to the goals and objectives laid out in their strategic plans. Assessing and prioritizing risks is an important step in operationalizing the strategic plan through the development of program plans, budgets, and the establishment of performance goals and controls.

In addition to the ERM guidance laid out in OMB Circulars A-11 and A-123, OMB provides guidance on integrating risk management practices in the management of Federal credit programs and non-tax receivables in Circular No. A-129. This includes guidance for risk management, data reporting, and use of evidence to improve programs through regular program reviews as well as establishing the Federal Credit Policy Council, an interagency collaborative forum for identifying and implementing best practices.

Finally, in September 2014, the Government Accountability Office (GAO) released an updated “Standards for Internal Control in the Federal Government” or “Green Book.” This document sets the standards for an effective internal control system for Federal agencies and provides the overall framework for designing, implementing, and operating an effective internal control system. It included new sections on identifying, assessing, and responding to risks.

II. Enterprise Risk Management Basics

A. Outcomes and Attributes of Enterprise Risk Management

ERM supports agencies' ability to articulate risks, align and allocate resources, and proactively discuss management and mitigation strategies and activities to better equip agencies to deliver on their goals and objectives and potentially improve stakeholder confidence and trust. ERM should operate with the purpose of:

- Supporting the mission and vision of the agency;
- Integrating existing risk management practices across functional silos;
- Improving strategic planning and decision-making;
- Improving the flow of risk information to decision makers;
- Including diverse viewpoints while driving towards consensus;
- Establishing early warning systems and escalation policies;
- Identifying, prioritizing, and proactively managing risks;
- Identifying opportunities;
- Supporting budget decisions and performance management;
- Establishing forums to discuss risks across functional silos;
- Promoting accountability and integrity of the agency's work; and
- Using a common approach to evaluating risks within the agency.

ERM should:

- Help bring clarity to managing uncertainty;
- Facilitate continual improvement;
- Be fully integrated into agency decision making processes, with active leadership support and engagement (i.e., setting the "tone at the top");
- Be tailored to the needs of the agency and take human and cultural factors into account;
- Build upon and unite existing risk management processes, systems, and activities;
- Be systematic, structured, and timely as well as dynamic, interactive, and responsive to change;
- Be based on the best available information; and
- Be responsive to the evolving risk profile of the agency.

B. Internal Controls and Risk Management

ERM and internal control activities provide risk management support to an agency in different but complementary ways. ERM is a strategic business discipline that addresses a full spectrum of an organization's risks and integrates that full spectrum into a portfolio view of risk. This encompasses all areas of organizational exposure to risk, as well as internal controls, which focus on operational effectiveness and efficiency, reporting, and compliance with applicable laws and regulations. ERM modernizes internal control efforts by integrating risk management and internal control activities into an ERM framework to improve mission delivery, reduce costs, and focus corrective actions towards key risks. ERM allows agencies to view their portfolio of risks as interrelated, helping to illuminate the relationship between key organizational risks and how and which controls can be used to mitigate or reduce risk exposure.

Key leaders should understand how their offices align with the risk management structure and be able to connect the dots across their agency's internal controls, compliance activities, and oversight functions. Agencies may find it useful to build an inventory that captures key oversight, compliance, and internal control activities, even those that are not formalized. For agencies that choose to establish a Risk Management Council or Committee (RMC), the resulting diagram could be used to help socialize this concept across the organization to help key leaders and staff understand the role of both the ERM organization and the RMC in relation to existing oversight activities as well as those still under development.

ERM Pitfall

Focusing too much on internal controls

ERM includes internal controls but also larger issues of the external environment, as well as transparency, business practices, reporting, and governance that help define the overall risk culture.

Coordinating ERM with other oversight activities in a complementary way will require both trust and collaboration between risk personnel and various oversight groups across the organization to ensure a proper understanding of their respective objectives and authority. It also requires a broad knowledge and subject-matter expertise by the team inventorying these activities, as well as an ability to identify and depict interdependencies among various groups. Table 1 highlights how traditional risk management activities complement ERM.

Table 1: Comparison between Traditional Risk Management and ERM

	Traditional Risk Management		ERM
	Risk Management (Project or Program)	**Internal Controls**	
Definition	Coordinated activities to direct and control an organization with regard to risk.[5]	A process affected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved.[6]	An effective agency-wide approach to addressing the full spectrum of the organization's significant risks by considering the combined array of risks as an interrelated portfolio, rather than addressing risks only within silos.

[5] Risk Management – Principles and Guidelines, International Organization for Standardization (ISO) 31000:2009

[6] Standards for Internal Control in the Federal Government (United States Government Accountability Office (GAO) Green Book)

The material in this document should not be construed as auditing guidance.

	Traditional Risk Management		ERM
	Risk Management (Project or Program)	**Internal Controls**	
Examples Highlighted in Federal Guidance	• Government Performance and Results Act Modernization Act (GPRAMA) of 2010 • Office of Management and Budget (OMB) Circular No. A-133 *Audits of States, Local Governments and Non-Profit Organizations* • *Risk Management Requirements for the Federal Acquisition Certification for Program and Project Managers* (FAC-P/PM)	• *Standards for Internal Control in the Federal Government* (GAO Green Book) • Federal Managers' Financial Integrity Act of 1982 (FMFIA) • OMB Circular No. A-123 *Management's Responsibility for Internal Control* • Chief Financial Officers (CFO) Act of 1990 • Federal Financial Management Improvement Act of 1996 (FFMIA)	• OMB Circular No. A-123 *Management's Responsibility for Internal Control and Enterprise Risk Management*(2016) • OMB Circular No. A-11 (Section 270) *Preparation, Submission, and Execution of the Budget*
Additional References	• Risk management – Principles and guidelines (ISO 31000:2009)	• Internal Control – Integrated Framework (COSO) • GAO Internal Control Management and Evaluation Tool	• Enterprise Risk Management – Integrated Framework (COSO) • Management of Risk - Principles and Concepts, "Orange Book" (Her Majesty's (HM) Treasury (United Kingdom))
Focus	Selected risk areas and processes generally focused on waste, fraud, and abuse within Federal Programs (e.g., grants management, program-specific risks).	Selected risk areas and processes generally governed under compliance activities and assessments (e.g., financial management, information technology).	Enterprise-wide and across every level taking an entity-level portfolio view of risk.
Emphasis and Application	Performance management against scope, time, and cost, as well as identifying and organizing program-level risks (e.g., risk registers organized by likelihood and impact).	Conforming to external reporting requirements (e.g., audit reports, identified material weaknesses). A siloed approach to assessing effective operations, reliable financial reporting, and compliance.	The use and application of risk information to improve decisions related to strategic planning, budgeting, and performance management across programs and activities.

The material in this document should not be construed as auditing guidance.

	Traditional Risk Management		ERM
	Risk Management (Project or Program)	Internal Controls	
Key Differences	• Risks are traditionally based on program or project operational execution, with risk tradeoffs made across cost, schedule, and performance. • Focus on risks is more forward looking than with internal controls, but does not extend beyond scope of program or project. • Some risk integration can occur, but may not extend past the program or project level. • Risk appetite and tolerance is usually not explicitly addressed. • Requires domain and technical program or product expertise, in lieu of functional experience.	• Primarily addresses traditional financial, compliance, transactional, and operational risks, with a focus on risk reduction through the application of discrete controls. • Risk assessments traditionally review past performance and activities and are generally not forward looking. • Risks are identified and managed on a siloed, non-integrated basis (e.g., financial reporting, human resources, physical security). • Risk appetite and tolerance is not addressed. • Requires specialized, functional skillsets (e.g., financial accounting, IT security).	• Addresses the full spectrum of an agency's risk portfolio across all organizational (major units, offices, and lines of business) and business (agency mission, programs, projects, etc.) aspects. • Provides the potential for a fully integrated, prioritized, and forward-looking view of risk to drive strategy and business decisions. • Allows for more risk management options through enterprise-level tradeoffs, versus a primary focus on reducing risk through controls. • Explicitly addresses risk appetite and tolerance. • Requires more general and interdisciplinary skillsets, rather than functional and domain knowledge.

C. Common Risk Categories

An effective ERM program promotes a common language to recognize and describe potential risks that can impact the achievement of objectives. Such risks include, but are not limited to strategic, compliance, credit, market, cyber, legal, reputational, political, model, and a broad range of operational risks such as information security, human capital, business continuity, and related risks. ERM addresses these risks as potentially interrelated and not confined to an agency's silos. Also, some risks may fall into multiple categories. A comprehensive list of common risk categories and their definitions are included in

Appendix A. This list is in no way complete but serves as an example of some of the risks an agency may face. It is important to not allow the categorization of risk to become a new silo for reviewing risk. Organizations should define risk categories in a way that supports their business processes and should use these categories consistently. Agencies may also consider developing a common risk language dictionary—a glossary of key risk terms to ensure all parties are consistent in their understanding of key concepts, words, and ideas. Categories of risk evolve over time, with new types of risk becoming salient and other risks becoming relatively less important.

D. Principles of Enterprise Risk Management

Part of developing an agency's risk culture is to agree on basic underlying principles. These can be used as regular reference points to gauge the extent that an agency is making progress. Moreover, these principles should be embedded in the approach of senior management in setting the "tone from the top."

1. **Governance Framework is Important:** ERM is built around a purposeful governance framework supported by the most senior levels of the organization and embedded into the day-to-day business operations and decision-making of the agency. Agencies may choose to adopt particular standards or frameworks (for example, COSO or ISO 31000), but it is important that whatever framework is selected, the agency customizes it to meet the mission, needs, structure, and culture of the organization. More important than compliance with any ERM framework is the ability to demonstrate that risks are managed in a way that supports good decision-making and meets its agency objectives. A framework should be forward-looking with assessments concerning maturity of the ERM program along the way.

2. **Managing Risk is Everyone's Responsibility:** Risk management enables understanding and appropriate management of the risks inherent in agency activities. It does not eliminate risk. While agencies cannot respond to all risks related to achieving objectives and goals, they should work to the extent possible to identify, evaluate, manage, and where appropriate, address challenges related to mission delivery. Risk management training should be available to all staff so they are equipped to manage risks associated with their work. Managers at each level should be equipped with appropriate skills and resources to manage risk appropriately. Further, agencies should put in place clear lines of communication for employees at all levels to identify areas of concern/potential risk and encourage such open communication to escalate reports of risks and bring them to the attention of the appropriate decision makers without repercussions.

3. **Managers Own the Risk:** Responsibility for success at each level of the organization means responsibility for managing risk at that level. For example, agency executives are responsible for the agency's enterprise risk, program managers own risks to their programs, and project managers are responsible for managing risks to their projects. The managers of government programs and activities should understand and take ownership of risks to achieving program outcomes, including both inherent risk and the tradeoffs of strategic decisions. Making risk-informed decisions requires that program managers articulate these risks and opportunities and to the extent possible manage risk in their portfolio across the organization. If an

agency creates a distinct ERM office, this is a second line of defense that creates a partnership with agency leadership and program managers to help them understand and manage their risk within acceptable levels, rather than taking responsibility for managing risks directly.

4. **Transparency Supports Informed Decision Making:** Informed decision making requires the flow of information regarding risks and clarity about uncertainties or ambiguities, up and down the hierarchy and across silos, to the relevant decision makers so they can make informed decisions. It is vital to create a culture where employees are comfortable raising risk-related concerns to senior managers and discussing risk openly and constructively – especially when parties disagree. Part of transparency is the need to report information so that decision-makers have a clear view of risks within and across silos. The reporting of "bad news" should become the way an agency does business rather than an act of courage by a lower-level employee.

5. **Forums for Discussing Risk are Important:** Agencies need to establish forums or committees to facilitate an open discussion of risk. Members should include policymakers, program leaders and risk management professionals within the agency, not just risk executives speaking to each other. Discussions of risk should include those both within and across silos in agencies. Forum structure will vary by agency. However, it is important that there be a mechanism in place to funnel important risk information up to the senior management of the agency or to the ultimate relevant policy maker.

6. **Risk Management Should Be Integrated into Key Agency Processes:** The risk management process should be integrated within organizational processes such as strategic planning, budgeting, and performance management. Agencies should consider risks from across the agency and use them as important inputs to these processes.

7. **Establishing Risk Appetite is Key:** Risk is unavoidable and sometimes inherent, as is the case with a credit program, in carrying out an organization's objectives. Agencies should evaluate, prioritize, and manage risks to an acceptable level. Clearly expressed and well communicated risk appetite statements establishing thresholds for acceptable risk in the pursuit of objectives are important. These statements help agencies make decisions about potential consequences or impacts to other parts of the organization, limiting unexpected losses.

   Defining risk appetite needs to be both a top-down and bottom-up exercise. The most senior members of an organization should define overall acceptable levels in conjunction with goals and objectives, and within the context of established laws, regulations, standards, and rules. Risk appetite helps to align risks with rewards when making decisions. Agencies can accept greater risks in some areas than in others. Each program establishes risk appetite levels that, when consolidated, are within the risk appetite boundaries established for the entire organization. Risk appetite can be implicitly established and communicated when setting strategic or operational goals and objectives. These levels may be expressed qualitatively or as quantitative metrics. They can also be explicitly set and communicated through targets associated with performance measures and indicators.

The material in this document should not be construed as auditing guidance.

8. **Existing Risk Analysis Models Are Important Within Limitations:** Standard risk management tools, including models and stress testing, can be important tools for measuring risk in a particular program. These tools can be used to show how the impact of an event could affect an agency's ability to achieve one or more of its objectives or performance goals. As helpful as risk tools can be, they are supposed to help inform decisions not to make them outright. Every model has simplifications that attempt to define reality and, thus, all have imperfections. It is important to understand these imperfections and to use a number of different models and approaches where possible.

9. **Planning Fosters a Culture of Resilience:** Risk management needs to be forward looking, learning from past mistakes as well as current best practices. This includes modeling severe downside scenarios and potential responses, as well as foresight planning exercises that consider what could go wrong, external factors that could impact mission achievement, gaps or short-comings in current business processes and resources, and other considerations. Developing strategies to respond to alternate future scenarios facilitates a culture of resilience, where programs can continue to meet objectives in the face of changing realities.

10. **Diversity of People and Thought Aids Risk Management:** The importance of bringing together different views and perspectives to discuss issues across various departments and programs (and not just within each program or department) is one of the lessons learned from the 2008 financial crisis. Risk management is about getting the right people around a table to discuss risk from various perspectives. This requires diversity of thought, which is greatly enhanced by a diversity of people, opinions, and perspectives. Agencies can benefit from diversity across all demographics in risk management discussions – including ethnic, gender, generational, geographic affiliation, educational, occupational and other factors.

E. Maturity of ERM Implementation

Implementing ERM throughout an agency requires careful thought and consideration about the best structure for the ERM function and where it should be located in the organization. Every organization has its own level of organizational and process maturity. These levels can be assessed using capability maturity models. An organization matures as it progresses from having no structure or doing ad hoc work to an optimized or leadership structure. A more mature risk organization will not only react to issues that arise but will be able to articulate the risks it faces and have in place management strategies to respond to those risks. It will look forward and try to predict what could happen and develop strategies to meet those contingencies. It will have risk dialogue within and across silos. In essence, a more mature risk organization will help create a culture which embodies the principles

ERM Pitfall

Too much too quickly

ERM is an iterative effort that develops over time. Management may consider an incremental approach, initially focusing on the top two or three risks or a type of risk. Success in a specific area can illustrate the benefits of ERM and build the foundation for future efforts. Trying to change the fabric of an agency too much or too quickly could result in defensive mechanisms within the agency hampering ERM efforts.

The material in this document should not be construed as auditing guidance.

discussed in this Playbook. Evaluating and improving the ERM of an organization is a long-term process that needs to develop and change over time and will be shaped by the unique needs, formal and informal decision making structures, culture, capacity, and mission of the organization. Examples of maturity models are available in Appendix B.

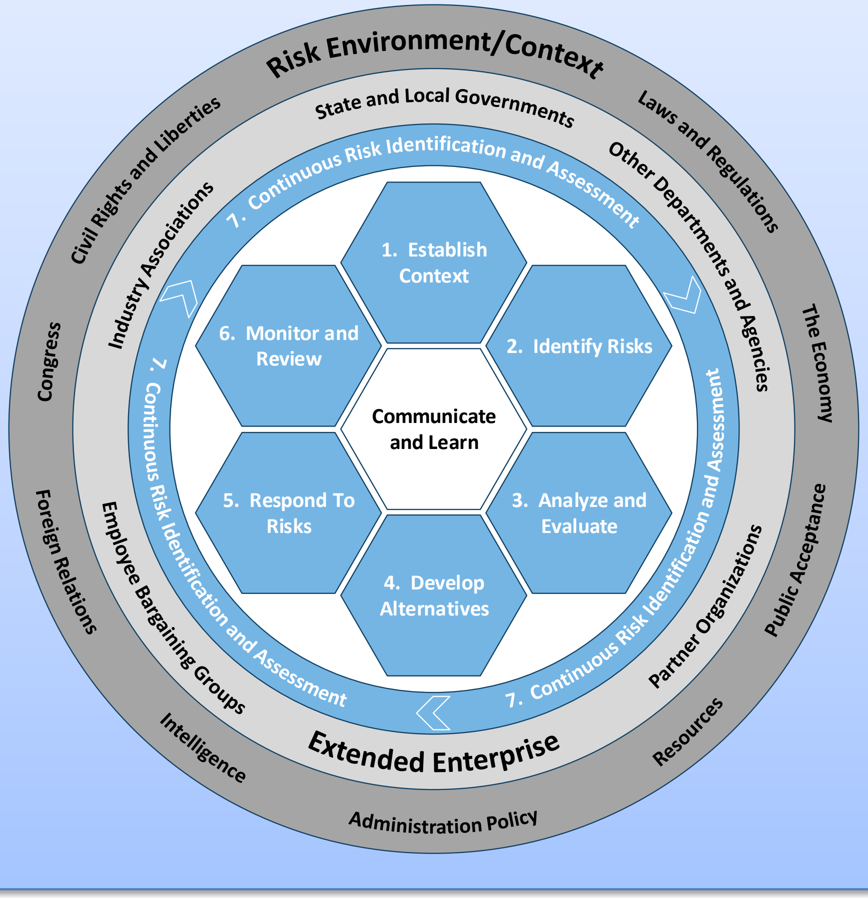
III. ERM Model

Each agency will need to determine how it will implement a comprehensive ERM program. Various frameworks may be considered as resources when making this determination including: 1) The Committee of Sponsoring Organizations of the Treadway Commission (COSO)'s *Enterprise Risk Management Integrated Framework* (September 2014); 2) ISO 310000; and 3) The United Kingdom's *Orange Book: Management of Risk – Principles and Concepts* (October 2004). ERM programs should be tailored to meet the individual needs of the agency or organization, and different components of these frameworks may be considered where most appropriate. Examples of ERM Frameworks are available in Appendix B.

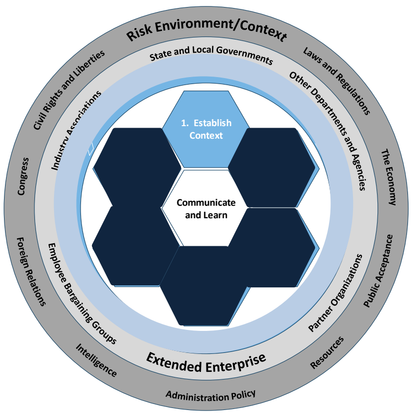
When considering these various frameworks, there are some common elements and phases of ERM that all approaches or models should include. These common elements are depicted in Figure 2: Illustrative Example of an ERM Model. Among them are: consideration of the context/environment; risk identification; analysis and evaluation; prioritization of risks; development of alternatives; risk response; and monitoring of implementation and outcomes.

It is important that whatever risk management approach is adopted, it be responsive to the unique needs and culture of the organization. The purpose is to assist those responsible for particular efforts in understanding, articulating, and managing risks. To complete this circle of risk management, the agency should incorporate risk awareness into the agency's culture and ways of doing business.

Figure 2: Illustrative Example of an ERM Model



A. Step One: Establish Context



Every agency functions within an environment that both influences the risks faced and provides a context within which risk has to be managed. Further, every agency has partners that it depends on for the delivery of its objectives. Effective risk management needs to give full consideration to the context in which the organization functions and to the risk aspects of partner organizations.

This broader risk context includes all factors that affect the ability of an agency to achieve its stated mission and program objectives, both internal and external. This includes but is not limited to Congress, the economy, the agency's capacity, legal and compliance structures; inter-dependencies with other agencies, partner organizations, and individual taxpayers; and expectations placed on the agency by the public.

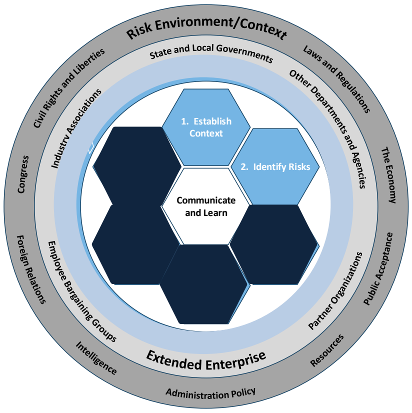
The first step in establishing the context is to determine the requirements and constraints that will

The material in this document should not be construed as auditing guidance.

influence the decision making process, as well as key assumptions. This involves taking into account policy concerns, mission needs, stakeholder interests and priorities, agency culture, and the acceptable level for each risk, both for the agency as a whole and for the specific program. Program managers should identify the control environment, delineating the safeguards in place to ensure compliance with applicable laws, regulations and policies. Finally, agencies should consider how relevant stakeholders, such as partner organizations, other departments and agencies, other levels of government, industry associations, employee bargaining groups, Congress, the Judicial Branch, internal and external auditors, sovereign entities, vendors, and the public interact with the program.

Understanding and defining the context will inform and shape successive stages of ERM implementation. Key components that should be considered, depending on the scope, timeline and complexity involved are described in Appendix C.

B. Step Two: Identify Risks



Agencies should use a structured and systematic approach to recognize potential risks and should strive to address all key risks significant to the achievement of organizational objectives. As the ERM process becomes more formal, agencies may want to adopt a risk register in which major risks are listed and their management is documented. The identification of risk may be an exercise conducted “top-down,” “bottom-up,” or both. In its most basic form, developing an agency risk register is an exercise through which managers and staff at each level of the organization are asked to list and articulate their major risks (i.e., “What keeps you up at night?”). Managers and subject matter experts, who are closest to the programs and functions and most knowledgeable about the risks faced, should serve as the primary source for identifying risks. The ERM office or program can provide useful assistance throughout the risk management process, through its unique background and view into the agency. After the listing of major risks is complete, agencies should examine them and decide which are the most significant risks to the agency (e.g., prioritize the risks based on likelihood and impact), and use the highest ranked risks to create the agency’s risk profile. Agencies also should consider risk velocity. Some risks, such as disinvestment in systems, may take a long time to cause major harm while others, such as a systems failure, can cause harm precipitously. For a list of key questions to help develop a risk profile and examples of risk profile formats, refer to Appendix D.

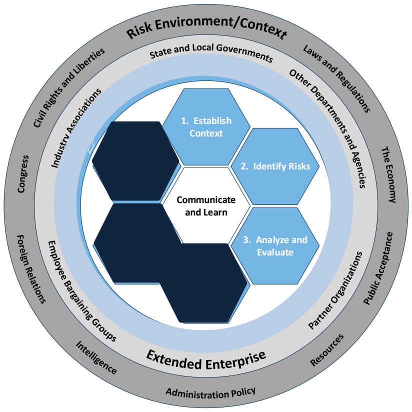
The material in this document should not be construed as auditing guidance.

Tips for Documenting Risks

1. **Develop meaningful risk categories:** When defining or categorizing risks, agencies should consider categorization in ways that are most helpful and relevant to agency mission. Agencies should be cautious to not limit categories only within silos or to neglect categorizing sources of risks not typically associated with a particular silo, while recognizing any single risk may be associated with more than one category.
2. **Use common language:** Risks should be described using a common language that resonates within the agency regardless of program office or individual expertise. Removing jargon whenever possible improves communication.
3. **Document risks regardless of control:** Agencies should consider the risks that are both within and outside of an agency's direct control, including third parties, vendors, or contractors, but present a genuine risk to an agency's mission. For major risks outside of the agency's direct control, often the only response may be to prepare contingency plans.
4. **Document action plans and outcomes:** It is important for agencies to document what was done to respond to possible risks and use these as lessons learned that can be leveraged for future strategic planning and response plans for new risks that may arise.

C. Step Three: Analyze and Evaluate

Once managers identify and categorize risks, agencies should consider the root causes, sources, and probability of the risk occurring, as well as the potential positive or negative outcomes, and then prioritize the resulting identified risks.

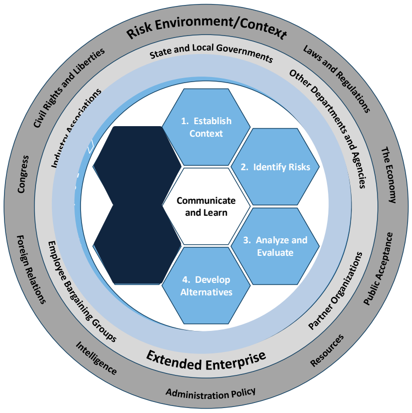


As part of the evaluation of risks, it is essential for agencies to reflect that risk can be an integral part of what agencies do. As an example, Federal credit programs are designed to meet specific social and public policy goals by providing financial assistance to borrowers who may be too risky to obtain private sector credit under reasonable terms and conditions from lenders. Perceived risks can be a large factor in the private sector's unwillingness to participate in the transaction but the government chooses to step in with specific credit program objectives because the potential social benefits and objectives are considered to outweigh the risks. Agencies should appreciate inherent risk within their programs or operations and incorporate them into their analysis and assessment of overall risk.

The material in this document should not be construed as auditing guidance.

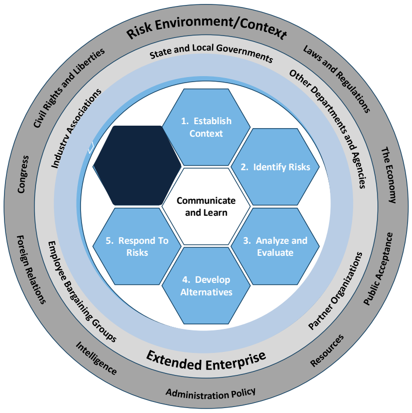
Assessments of the likelihood and impact of risk events help agencies monitor whether risk remains within acceptable levels and support efficient allocation of resources to addressing the highest-priority risks. Agencies can be too risk-averse. It is important to assess risks of standing still and either missing opportunities or becoming vulnerable to a changing environment. Examples of risk assessment tools can be found in Appendix D.

D. Step Four: Develop Alternatives



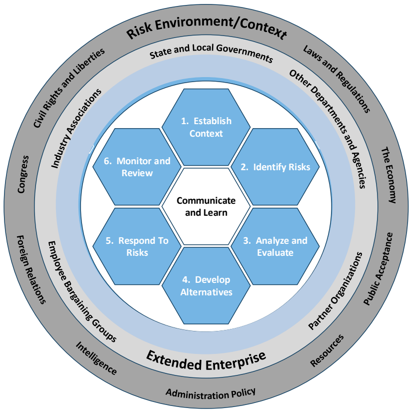
Guided by risk appetite, agencies should systematically identify and assess a range of response options or strategies to accept, transfer, share, avoid, or mitigate major risks. Compare the cost of addressing the risk with the risk of exposure, the value of potential benefits and losses, and determine how to allocate resources accordingly. Consider non-financial costs in terms of the reputational or political capital at stake. Also evaluate control options to respond to risk which may be preventative, corrective, directive, or detective in design.

E. Step Five: Respond to Risks



After identifying and analyzing major risks, prioritizing them, and developing appropriate strategies to address the highest priority risks, the agency leadership must decide how to allocate scarce resources, such as budget resources, analytical capabilities, and management attention, to address them. While the risk officer or risk office can help to facilitate the process, managing risk is the responsibility of the unit heads where the risk resides. Once risks are prioritized and risk responses are determined, milestones for carrying out the risk management process should be documented. The risk officer or office should then monitor implementation of the risk management strategy to ensure that it is being carried out effectively and in a timely manner. Agency leadership may need to adjust the approach to managing particular risks if implementation somehow fails to bring the risk within desired limits.

F. Step Six: Monitor and Review



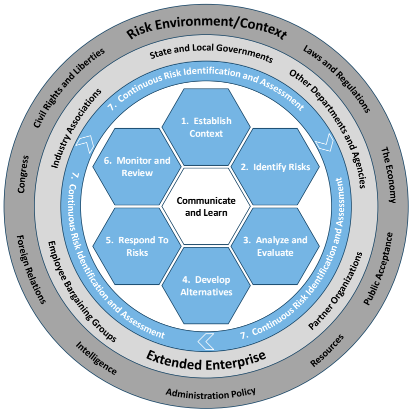
Agencies should regularly review, monitor, and update (as necessary) risk information documented within the enterprise-level risk profile to identify any changes and determine whether risk responses and mitigations are managing risks as intended. This review should occur semi-annually at a minimum. As part of this ongoing process, risk personnel should work with senior leadership to determine if originally identified risks still exist, identify any new or emerging risks, determine if likelihood or impact has changed, and ascertain the effectiveness of controls or mitigants put in place. It is a good practice to regularly review and update risk data at all levels of the agency as appropriate. Any significant changes to the risk profile should be escalated to the appropriate senior leader for discussion and should be made part of the agenda for discussion with the RMC.

It is expected that this step will result in a risk register, dashboard, or other report to communicate the status of risk response activities. This includes whether an action has been started, completed, or delayed, and whether the action taken had the desired effect on the risk. It can also show what the residual risk is and where additional response is required. Monitoring efforts may include assigning responsibility for implementing risk responses (usually it lies with the manager where the risk resides); setting milestones and criteria for success, and monitoring to ensure the intended actions are completed. Examples of risk communication tools are available in Appendix E.

Progress in implementing risk response strategies provides a performance measure. The results can be incorporated into the organization's overall performance management, measurement, and external and internal reporting activities.

G. Step Seven: Continuous Risk Identification and Assessment

Risk identification and assessment should be an iterative process, occurring throughout the year, including surveillance of leading risk indicators both internally and in the external environment. Once ERM is built into the agency culture it can be possible to learn from managed risks, near misses when risks materialize, and adverse events, and can be used to improve the process of risk identification and analysis in future iterations. All aspects of ERM, including formal tools such as risk profiles and statements of risk appetite need to be regularly reviewed and evaluated to determine whether the agency’s implemented risk management strategies are achieving the stated goals and objectives, whether the identified risks remain a threat, whether new risks have emerged, and how ERM processes can be improved.



Integrating risk management into existing agency planning, performance management, and budget processes is essential if ERM is to be effective. Agency strategic plans, for example, should reflect an assessment of current and future risks to mission achievement and plans for how the agency may respond to such eventualities including risks of standing still while the context changes. The Government Performance and Results Act Modernization Act (GPRAMA) requires that agencies revise strategic plans every four years and assess progress toward strategic objectives annually. Incorporating a review of the risk appetite and identified risks associated with each objective into this process encourages an ongoing dialogue about risk and performance. Finally, integration with the budget process is needed so that the agency seeks to allocate its scarce budget resources to address the highest priority risks preferably before adverse events materialize.

The material in this document should not be construed as auditing guidance.

IV. Developing an ERM Implementation Approach

Agencies should develop plans for implementing ERM into management practices. The planned approach to implementing ERM should include a planned risk governance structure, processes for considering risk appetite and tolerance levels, methodology for developing a risk profile, and general implementation timeline and plan for maturing the comprehensiveness and quality of the risk profile over time.

It will be up to each agency to decide the best way to complete each of these plans. Because every agency is different, each will have a different way that it wishes to create a risk management governance structure and develop a risk appetite and risk profile. Links to examples of implementation plans are available in Appendix C.

V. Risk Governance

A strong culture of risk awareness is needed throughout the agency. This culture can only occur if top agency leaders champion ERM and the flow of information needed for effective decision making. Risk management training, risk assessments conducted collaboratively with operational and program staff, agency-wide communications about the importance of risk identification and management, performance incentives that encourage risk management, and regular reports identifying significant risks across the agency all can help build the needed culture. A strong ERM governance structure and program will significantly help agency leaders make risk-informed decisions about resource allocation, policy, and operations that can lead to improved mission performance and agency resilience to changes in internal and external factors.

ERM Pitfall

Absence of support from senior leaders

Strong leadership at the top of the organization, including active participation in oversight, is extremely important for achieving success in an ERM program. ERM also requires active involvement and commitment from leaders in each business and program area (i.e., across silos) to develop and maintain a risk aware culture.

As an agency develops its risk governance structure it is important that it promotes communication and consultation with stakeholders. This will result in the identification of risks and response strategies that include the perspectives of program managers and key stakeholders. The governance structure needs to be built on the understanding that stakeholders can be internal or external to the agency. Agencies should consider the desired outputs of communication and consultation, and decide where in the risk process to engage stakeholders. Communications can include formal and informal meetings with internal and external stakeholders, verbal or written reports, surveys, or emails, and meetings with teams to address specific risks, programs, objectives, or leadership

The material in this document should not be construed as auditing guidance.

activities. Part of the ERM process will be to define and establish documentation requirements and reporting methods.

Effective risk governance requires continuing and focused support from the top of the organization. One effective approach is to create a RMC, chaired by the COO or a senior official with responsibility for the enterprise. In Cabinet level agencies, this is the Deputy Secretary. The RMC should meet regularly (e.g., monthly) to consider a range of major risks. It is essential that senior leadership be willing to respond to important risks identified and prioritized by the committee by making decisions about how to respond to a risk and then allocating the needed resources (in terms of budget, staffing, or management attention, for example) to ensure that the risk is properly addressed. If the RMC limits its dialogue to identifying and prioritizing risks without implementation of effective responses it will quickly become an empty forum for discussion rather than a source of value in addressing major risks.

ERM Pitfall

Lack of a core team

Hiring one individual to stand-up the ERM program for a mid to large size agency is problematic. Each agency should assess the level of support necessary to implement and manage ERM effectively. To be effective, the ERM program will need the appropriate team with knowledge and experience in risk management, leadership, and gravitas to build the ERM function. If an agency does not have a CRO or intend to hire one, it should also carefully consider where the core team fits in the agency to make it most effective. While agencies should be careful about building an ERM empire, the size of the ERM team should reflect the needs of the organization to support effective risk management.

An effective governance structure for ERM, internal controls, and performance management would define the roles, responsibilities, and ownership of these functions and ensure they complement each other. In defining the ERM governance structure, leadership and those in the risk management role should think about how to leverage existing risk management activities and coordinate with current efforts in the organization for reviewing strategic direction and goals such as quarterly performance reviews and the Strategic Objective Annual Review (SOAR) required by GPRAMA.

Examples of ERM governance structures, roles and responsibilities, and risk governance committee charters are available in Appendix B.

VI. The Risk Appetite Statement

A. What is Risk Appetite

As noted earlier, risk appetite is the amount of risk an organization is willing to accept on a broad level in pursuit of its objectives given consideration of costs and benefits. Without closely considering risk appetite, an organization may take more or less risk than may be appropriate to achieve the associated

The material in this document should not be construed as auditing guidance.

gains. Clearly expressed and well-communicated risk appetite statements can provide guidance on the amount of risk that is acceptable in the pursuit of objectives and can help policymakers make informed decisions. These statements help agencies make risk-informed decisions with regard to allocation of resources, management controls, and potential consequences or impacts to other parts of the organization, and can reduce surprises and unexpected losses. Again, a practical approach is recommended. Discussing qualitative aspects and general appetite for risks materializing is more important than trying to apply a quantitative formula or mathematical precision regarding such risks.

B. Relationship Between Risk Appetite and Strategic Objectives

Risk appetite should be informed by the public policy purpose of the program and the agency's mission as well as the environment in which it operates. For example, if the stated objective of a program is to encourage home ownership, agencies may tolerate a higher risk of default when backing mortgage loans for low-income borrowers than would be suitable for a private lender. However, if the desired result of the program emphasizes *access to affordable, high quality housing* (including rental housing), rather than home *ownership,* the acceptable risk of default may be much lower, which means a lower risk appetite. Similarly, if the purpose of a program is to inject capital into an under-served market during a recession in which private lenders are "de-risking", or cutting back on lending to high-risk borrowers, the government may determine a higher risk of default is acceptable at that point in order to fulfill that market need. In this case, the government would have a higher risk appetite than in more expansive times.

C. Considerations When Developing Risk Appetite

Agencies should visualize the relationship among likelihood, impact, and tolerability of risk and consider the relative severity of each risk in terms of impact on the mission objective. In doing so, agencies may adopt rating scales, such as a scale ranging from 1-5, and set relative differences across the levels.

Risk appetite levels should be developed by merging ideas both top-down and bottom-up, with top leadership approval of the final risk appetite statement. The most senior members of an organization should be involved in setting overall risk appetite levels in conjunction with goals and objectives. Risk appetite should be considered within the context of established laws, regulations, standards, and rules. Each program should also set out its own individual risk appetite level so that all of the individual levels, when consolidated, fall within the appetite for the entire organization.

VII. Developing a Risk Profile

OMB Circular No. A-123 requires each agency to develop a "risk profile." Circular No. A-123 defines a risk profile and its purpose in the following terms:

> *The primary purpose of a risk profile is to provide a thoughtful analysis of the risks an Agency faces toward achieving its strategic objectives and arising from its activities and*

The material in this document should not be construed as auditing guidance.

> *operations. The risk profile assists in facilitating a determination around the aggregate level and types of risk that the agency and its management are willing to assume to achieve its strategic objectives.*

The risk profile differs from a risk register in that it is a prioritized inventory of the most significant risks identified and assessed through the risk assessment process versus a complete inventory of risks.

A. Steps to Creating a Risk Profile

When developing a risk profile or a listing and assessment of the agency's top risks, agencies will want to ask themselves questions each step of the way so that the risk profile will be tailored to their agency's circumstances. Examples of questions agencies may consider as part of developing a risk profile are available in Appendix D. The answers to these questions will enable agencies to identify the most significant risks, assess those risks, and determine appropriate response strategies.

There is no single best way to document an agency's risk profile and agencies will have discretion in terms of the appropriate content and format for their risk profiles. However, Circular No. A-123 calls for agencies to include the following seven components:

1. Identification of Objectives
2. Identification of Risk
3. Inherent Risk Assessment
4. Current Risk Response
5. Residual Risk Assessment
6. Proposed Risk Response
7. Proposed Action Category

Although it is logical that these seven components will often be involved in risk analysis at all levels of an agency, it is important to note that for purposes of A-123 these seven components only need to be documented for the major risks at the overall Agency level in preparation of their discussion with OMB.

Step One: Identification of Objectives
Agencies should begin by identifying their objectives. There are four objective categories outlined in OMB's Circular No. A-123: strategic, operations, reporting, and compliance. These four categories also align with the Objective Setting component of the COSO ERM Integrated Framework. The categories provide guidance on the intended scope of the objectives which should be defined as part of the agency process, but agencies do not necessarily need to use these four objective categories for their analysis. Per COSO, some organizations develop risk categories based upon the categorization of their objectives, using a hierarchy that begins with objectives relevant to organizational units, functions, or business processes. OMB Circular No. A-123's four objective categories and corresponding definitions are outlined below, as well as more enhanced definitions relating to corresponding risk areas that may align or overlap with each objective category.

The material in this document should not be construed as auditing guidance.

Table 2: Objectives as outlined in Circular No. A-123 and their corresponding risk categories

A-123 Objective	Corresponding Risk Category
Strategic: Relating to the strategic goals and objectives aligned with and supporting the agency's mission	**Strategic Risk:** The risk of failing to achieve strategic or tactical objectives because the strategic and tactical planning process, leadership, or implementation of the strategic plan is not fully effective. Strategic risks can be affected by changes in the political environment such as changes in administration and resulting changes in strategic priorities. Strategic risk can also be triggered by actions of key stakeholders such as other Federal agencies or by law makers as described in the definition of political risk. When thinking about strategic risk, agencies should also consider the concept of effectiveness – the ability of agencies to demonstrate and measure the effectiveness of a particular program.
Operations: Relating to the effective and efficient use of the agency's resources related to administrative and major program operations, including financial and fraud objectives	**Operational Risk:** The risk of direct or indirect loss or other negative effects on an agency due to inadequate or failed internal processes, or from external events that impair internal processes, people, or systems. Operational risk encompasses a broad range of risks (e.g., legal, compliance, and other risk types identified in this section, as well as business continuity, business processes, human capital, and technology) which can have a direct impact on daily operations of an agency. Included in operational risk is reporting risk – the risk associated with reliability of reporting information needed to manage the agency and monitor its progress.
Reporting: Relating to the reliability of the agency's reporting	**Reporting Risk:** The risk associated with the accuracy and timeliness of information needed within the organization to support decision making and performance evaluation, as well as, outside the organization to meet standards, regulations, and stakeholder expectations. This is a subset of operational risk.
Compliance: Relating to the agency's compliance with applicable laws and regulations	**Compliance Risk:** Failure to comply with applicable laws and regulations and failure to detect and report activities that are not compliant with statutory, regulatory, or organizational requirements. Examples include laws and regulations governing procurements and Federal assistance, privacy statutes and regulatory requirements. Compliance risk includes risks resulting from a lack of awareness or ignorance of the pertinence of applicable statutes and regulations to operations and practices.

Some key questions agencies should consider during this step are as follows: What are our objectives? What do we need to consider when we assess the risks of achieving our objectives? What criteria will we use to assess our risks? Who will conduct the assessment? How will we validate the quality of our risk profile?

Risk exists only in the context of trying to achieve something. At the enterprise level, it may be a vision, a mission, a set of strategic goals, a legislative imperative, or a mix of these. At the program, project, or

The material in this document should not be construed as auditing guidance.

transaction level, objectives will be more narrowly defined, but they should be explicit. Objectives may be defined by level (enterprise, program, project, transaction) or by category (strategic, operations, compliance, reporting).

Additionally, both the internal and external environments in which the agency seeks to achieve its objectives should be considered. A Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis, which is also useful for analyzing the external environment, can be helpful in analyzing internal factors. External considerations include but are not limited to stakeholders, including elected officials and the public; legal and regulatory requirements; economic and financial considerations; technological capabilities; and requirements and trends that impact the organization’s objectives. Internal considerations include anything within the organization that can influence the way in which the agency will manage risk such as mission, culture, structure and governance, goals and objectives, risk tolerance, performance metrics, resources, internal stakeholders, information systems, decision making processes, policy, standards, and guidelines.

By the end of this step you will have clarified the enterprise, program, office, or other objectives for which you are assessing risk. You should have an understanding of the internal and external environment in which you are trying to achieve those objectives. You should know what approach you will use to identify risk, who will be involved, and the criteria you will use to assess risk.

Step Two: Identification of Risk

In this step, an agency will generate a list of the barriers (threats) and enablers (opportunities) to achieving its objectives. Risk management is an art more than a science. This step is the art of turning threats and opportunities into risk statements. This is a way of verbalizing what it is agencies are making decisions about and why.

Information captured for each risk should include the related strategic objective, if applicable, whether or not the risk is in fact a control deficiency or high-risk area previously identified, and any remediation plans, corrective actions, or mitigation strategies for the risk. The assessment process should consider both positive and negative risks and may focus on information collected from previous reports and sources, such as those in the following list.

The material in this document should not be construed as auditing guidance.

Sources for Identifying Risks

- **Agency Reports and Self-Assessments**
  - Previous year Federal Managers and Financial Integrity Act reports and A-123, Appendix A self-assessments and related assurance statements. Specifically, this may include:
    - Entity-level control interviews and evidence documentation;
    - Assessment of agency processes and thousands of documented controls;
    - Documentation of control deficiencies, including the level of significance of those deficiencies (simple, significant, or material weakness); and
    - Corrective actions associated with the deficiencies and tracked to either remediation or risk acceptance.
  - Financial Management Risks documented in the agency's Annual Report.
  - Project management risks documented in the agency's investment and project management processes.
  - Anything raised during Strategic Objectives Annual Review, quarterly performance reviews, RMC, etc.
- **Inspector General (IG) and Government Accountability Office (GAO)**
  - IG Management Challenges documented annually in the agency's AFR.
  - IG audits and the outstanding corrective actions associated with those audits.
  - GAO audits and the outstanding corrective actions associated with those audits.
- **Congress**
  - Issues and risks identified during Congressional Hearings and Questions for the Record.
- **Media**
  - Issues and risks identified in the news media.

Upon completing the initial identification of risks, an agency may wish to consider conducting an initial analysis of the compiled risk information and create a working list of risks based upon review of existing documentation above. This may serve as a preliminary list of risks to use during interviews with key stakeholders and other key personnel. Results analyses could then be conducted on a rolling basis throughout the risk identification and assessment process.

Agencies may wish to consider conducting interviews and discussions with key stakeholders and other key personnel. These interviews and discussions will help to validate the preliminary risk list and identify additional risk items. These interviews and discussions will also help to identify and document additional areas of known or emerging risk, current and proposed risk responses, and other relevant risk information including ratings for inherent and residual risk. Some key questions to consider during this step are: What current events or longer term developments are occurring that would affect my program areas or objectives? What are the corresponding impacts? How quickly will particular major risks cause an impact?

The risk officer can conduct interviews and facilitate workshops designed to generate information about major risks as perceived by people in all parts of the agency. From this consultative and interactive process, the risk office can generate a preliminary list of major risks or add to an initial risk list compiled from existing documentation, as discussed in the previous section. The nature of the risk identification process will affect the results and the time required to perform the analysis. Workshops with people from multiple disciplines may provide a more complete perspective but will require time and facilitation, compared to interviews only with key managers. Relying on a subject matter expert may seem efficient, but this may preclude consideration of a larger range of threats and opportunities, and especially those that are cross-cutting. Communication and consultation with partners or other stakeholders may provide mutual understanding and confirmation of preliminary determinations. Known risks identified from prior assessments should be vetted with key managers and stakeholders to address any changes in their context.

ERM Pitfall

Failure to work closely with program leaders

In building out an ERM program, it is best to work with those within the agency that already own and manage risk to gain insights into the most significant and relevant risks facing the organization. It is an ERM program's role and responsibility to provide risk management assistance to others in the agency, not the other way around. The ERM program's first questions to agency managers should always be: What are your major risks? And, how can we support you in better managing them?

A simple narrative statement should be developed to describe each major risk identified. The statement should give some context to the issue and describe the perceived impact from the risk. It may be helpful to use the "if/then" format to identify the risk events and the resultant impacts. Be sensitive to potentially serious risks that cut across organizational units so they do not get lost. Also consider possible linkages of events and risks.

It is expected that this step will generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate, or delay the achievement of objectives. An agency wants to strive to be as comprehensive as possible to avoid missing risks that should be included in further analysis. When identifying risks, an agency should consider and include risks whether or not their source is under the control of the organization. During risk identification, agencies should not just look vertically for risks, but horizontally across the agency and external partners to find risks that would affect achievement of agency objectives. Risk identification should include consideration of the secondary and cumulative effects of particular impacts. It should also consider a wide range of impacts even if the risk source or cause may not be apparent. It is necessary to consider all possible causes and scenarios so that all significant consequences are considered. This is not to say that multiple strategies need to be

The material in this document should not be construed as auditing guidance.

devised. Understanding all of the possible risks will help an agency develop a thorough response strategy.

Step Three: Inherent Risk Assessment

The preliminary risk list compiled as a result of risk identification activities will need to be analyzed to rate the inherent risk level based on impact and likelihood. Inherent risk is the exposure arising from a specific risk before any action has been taken to manage it beyond normal operations. Inherent risk is often referred to as "the risk of doing business". Impact refers to the effect of an event on strategic goals and objectives. Impact can be positive or negative related to the organization's objectives. Likelihood is the probability that a given event will occur.

These criteria should be used to assess the level at which a risk requires a response and the level of that response. To approach this process, it can be helpful to create a multi-disciplinary committee with representatives from major operating and mission units to assess the level of risk response. Sometimes it can be helpful to draw on subject matter experts, or involve external or specified internal stakeholders. Root-cause analysis can help an agency to link otherwise disparate occurrences and determine that a set of risks together may be more significant than they seemed at first. Agencies need to decide on the tools that seem most effective in identifying, assessing, and documenting major risks.

Examples of a three level rating scale for measuring impact and likelihood respectively, (taken from OMB Circular No. A-123) are shown below:

Table 3: Example of a Risk Impact Rating Scale

Rating	Description
High	The impact could preclude or highly impair the organization's ability to achieve one or more of its objectives or performance goals.
Medium	The impact could significantly affect the organization's ability to achieve one or more of its objectives or performance goals.
Low	The impact will not significantly affect the organization's ability to achieve one or more of its objectives or performance goals.

The impact assessment is used to gauge how large the impact will be. For example, is there a threat to human life? Is there a threat of fraud waste and abuse? Is there an opportunity for technology implementation? Is there an opportunity to meet strategic goals?

Estimate the level of impact based on what will happen if the event occurs. Make the assessment based on informed judgment of knowledgeable individuals and groups.

Table 4: Example of a Risk Likelihood Rating Scale[7]

Rating	Description
High	The risk is very likely or reasonably expected to occur.
Medium	The risk is more likely to occur than unlikely.
Low	The risk is unlikely to occur.

The likelihood assessment is used to gauge how likely an event is to occur. For example, events that may happen every day have a far greater likelihood than events that may only happen once in 10 years.

Estimate the likelihood based on data when available with a future projection or based on an expert's or a group's knowledge and assessment of the risk. Certain conditions may increase or decrease the likelihood of a risk event and its impact.   Another key aspect to keep in mind is risk velocity. While some risks such as disinvestment in a key system may materialize slowly, their impact could be substantial. Other risks, such as a systems failure, could materialize quite rapidly.

Agencies will assess their risks based on the impact of threat or opportunity being triggered and the likelihood of the event happening. Assessing risks gives agencies a way to better understand and prioritize them. Risk analysis involves consideration of the causes and sources of risk, their positive and negative impacts, and the likelihood that those impacts can occur. Given that risk assessment is more of an "art" than a science, it ultimately may depend on qualitative analysis, informed by discussions based on subject matter experience. It may be in some agencies, or for some programs within agencies, that quantitative risk assessments are appropriate to back up more qualitative assessments.

Identifying existing controls is an important step in the risk analysis process. Internal controls (such as separation of duties or conducting robust testing before introducing new software) can reduce the likelihood of a risk materializing and the impact. This step in the risk analysis process provides an opportunity to identify controls that may reduce risk. Audit reports and management reviews may provide useful reference points for this part of the analysis. One way to estimate the effect of a control is to consider how it reduces the threat likelihood and how effective it is against exploiting vulnerabilities and the impact of threats. Execution is key—the presence of internal controls does not mean they are necessarily effective.

Prioritizing risks will allow agencies to examine the impact level and likelihood resulting from the analysis step to help determine a relative importance and a priority ranking for risk. Creating a priority ranking communicates the most important issues on which you are making decisions. Not all of your priority risks will require actions. At this point it is recommended that you decide which risks represent your top risks without regard to resource constraints. What are the impact levels and likelihood of your risks? How do the risks compare, such as on a heat-map? How do the risks compare to your risk appetite? What risks do leadership consider "top risks?" What risks will require a response?

Sort your risks based on their likelihood and impact. A "heat-map" can be useful to for plotting risks based on the analysis results to visually compare risks. Decide which represent your top risks and assign

[7] Likelihood may be based on the risk occurring in a given period of time as determined by the agency.

a priority to each. The heat-map is only a tool and examples of heat maps are available in Appendix D. Leadership should validate the list of top risks and the supporting analysis results. Agency leaders can provide a perspective from the appropriate level of the organization to normalize information across objectives, programs, and performance areas.

Prioritized risks from across the enterprise can be aggregated to assist in developing an agency risk profile. Keep in mind that while risks have relative importance within programs or units based on their context, simply aggregating risks from across the organization does not indicate “enterprise” level risks. Senior leadership should evaluate and prioritize risk to the organization as a whole.

Step Four: Current Risk Response
Risk responses are the actions taken to manage or treat risks. Per Circular No. A-123, types of risk responses may include:

- **Acceptance:** No action is taken to respond to the risk based on the insignificance of the risk; or the risk is knowingly assumed to seize an opportunity.
- **Avoidance:** Action is taken to stop the operational process, or the part of the operational process causing the risk.
- **Reduction:** Action is taken to reduce the likelihood or impact of the risk.
- **Sharing:** Action is taken to transfer or share risks across the organization or with external parties, such as insuring against losses.

Current risk responses in place should be guided by an agency’s risk appetite and tolerance levels. In instances where appropriate risk responses included implementation of formal internal control activities, it is recommended that the risk group work with the A-123 Internal Controls team to ensure these risk items are addressed and included in the A-123 testing.

A-123 Requirement: Criteria for risks that require formal internal controls

- The Agency is working to reduce exposure to the risk.
- Internal control objectives related to reporting, compliance, or operations, including both administrative operations and the major operational components of programs.
- The risk is identified in the Agency risk profile as at least medium impact and medium likelihood (i.e., the risk is greater than low).
- Public reporting on the risk will not negatively impact services provided to the public, national security, or agency operations.
- Control objectives can be clearly specified.

As part of this step, agencies will need to decide whether to pursue a new strategy or continue with their current one based on program risk. Selecting the most appropriate risk response strategy involves balancing the costs and efforts of treatment against the benefits derived. Your risk response strategies will help you identify actions and priorities to be included in your performance plans.

Key questions to consider during this step include: What actions will be taken to avoid, mitigate, transfer, share, or accept our risks? Are these actions actually mitigating the risk? How long will the ongoing actions continue? Who is accountable for ensuring the success of these risk responses?

Current risk response strategies and activities should be documented within the risk profile. Avoiding or transferring risks may require little effort but should be documented to show there is a strategy in place.

Step Five: Residual Risk Assessment

Residual risk is the amount of risk left over after action has been taken to manage it using the same assessment standards as in the Inherent Risk Assessment. These risks should be communicated along with the other identified risks. These risks will tend to be addressed during the agency's ongoing updates of risk identification processes.

Finalizing the draft Agency Risk Profile

Upon completion of Steps 1 through 5, agencies should finalize the draft Risk Profile for discussion and vetting with senior leadership. As part of the finalization process, agencies will determine which risks should be included as part of their draft Risk Profile. Agencies should present their final draft Risk Profile to senior leadership for discussions and vetting. This draft Risk Profile may be shared with leadership on an individual basis, as part of a current standing meeting such as an Operating Committee Meeting, the Strategic Review process, or as part of the formal risk management governance process. Agencies should use their discretion when determining appropriate process and venue for sharing the draft Risk Profile. Once this vetting process has occurred, the draft Risk Profile should be formally shared with the risk governance body or RMC so that determinations can be made around additional proposed risk responses, risk owners, and proposed risk response categories.

Note: *The processes to develop annual assurance statements for FMFIA and A-123, Appendix A should consider the risks identified in the agency's risk profile, to the degree they are relevant. This will help to ensure that the assurances the agency COO, or equivalent, provides to the Department Senior Management Council, where applicable, includes consideration of all risks.*

Step Six: Proposed Risk Response

Proposed risk responses are actions planned or suggested to further reduce residual risk. After agency senior leadership have completed their review of the draft agency risk profile, it should be forwarded to the RMC or equivalent for deliberative discussion and consideration around additional actions (proposed risk response) that may be suggested or required to reduce the overall level of residual risk and align to the organization's risk appetite. An organization's risk appetite and tolerance levels must be clearly understood when considering and developing proposed risk responses.

The draft risk profile should be shared with the RMC in advance of any meeting to encourage greater discussion regarding additional proposed actions to further mitigate risk. It is also important for RMC members to understand their organization's complete draft risk profile when determining additional proposed risk response as they must be considered and prioritized in the context of the overall enterprise and its existing risk appetite.

The RMC or the agency head, as appropriate, should make the final determinations relating to appropriate management approaches and proposed actions based on the agency's risk appetite and tolerance levels.

A risk owner or primary accountable official or office, should be named for the additional proposed risk response. Naming a primary accountable official increases the likelihood that action will be taken.

Step Seven: Proposed Risk Response Category

The identification of existing management processes that will be used to implement and monitor the proposed actions is also required. This will promote a more organized approach to executing the proposed actions. Examples of proposed risk response categories might include: internal control assessment, strategic review, budget process, etc. Just as naming a primary accountable official increases the likelihood that action will be taken, naming a proposed risk response category will also help to ensure that additional proposed risk responses are being considered as part of the most appropriate processes.

B. Additional Considerations

Finalizing Risk Profile

The final risk profile differs from the draft risk profile in that it includes additional proposed risk responses, risk owners, and proposed risk response categories. The inclusion of this additional information assists with the ongoing tracking, review, and analysis of the achievement of additional proposed risk responses and ultimately the reduction of risk exposure to meet risk tolerance levels and better alignment to the organization's risk appetite.

Sharing Risk Profile Results with OMB

As discussed in Circular No. A-123, agencies should plan to make key information identified as part of the risk profile available for discussions with OMB by June 2, 2017 as part of the Strategic Review meetings and/or FedSTAT. The final determination on information to be shared with OMB will be provided in early 2017. This information will be communicated to agencies by OMB.

The material in this document should not be construed as auditing guidance.

VIII. GAO/IG Engagement

As stated in A-11 Section 270.28, ERM and audit functions perform two independent but complementary functions. ERM is a highly engaged yet independent source of holistic and dynamic risk assessment that supports program leads to help them better identify and manage their risks. As such ERM is considered a business line function. However, Federal auditors, namely the GAO and IG, are statutorily mandated to conduct independent and objective audits, evaluations, and investigations of an agency's programs and operations and its ability to manage risk. Both are designed to add value and improve an organization's operations.

The engagement between the risk and audit functions will be pursuant to a maturation process that will develop over time. Both groups have the same goal as the ERM function– better management of the organization – and, thus, a mature risk/audit engagement will see the creation of risk registers, risk assessments, and risk profiles by management as a valuable tool for advancing and protecting the mission of the organization. Also, as previously mentioned, the risk management function will benefit from audit findings that identify and assess additional risks.

IX. Appendices

The following appendices include a collection of examples and templates provided by various government organizations to support ERM implementation. They may be modified to fit the culture, circumstances, conditions, and structure of other agencies. The appendices are intended to be illustrative of what other agencies have done for ERM and are not intended to set the standard for audit or other compliance reviews.

Appendix Contents

A. Risk Types

Risk Type	Risk Description
Compliance Risk	Risk of failing to comply with applicable laws and regulations and the risk of failing to detect and report activities that are not compliant with statutory, regulatory, or organizational requirements. Compliance risk can be caused by a lack of awareness or ignorance of the pertinence of applicable statutes and regulations to operations and practices.
Credit Program Risk	The potential that a borrower or financial counterparty will fail to meet its obligations in accordance with their terms. If the credit exists in the form of a direct loan or loan guarantee, credit risk is the risk that the borrower will not fully repay the debt and interest on time.
Cyber Information Security Risk	Risk that could expose the agency to exploitation of vulnerabilities to compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by its information systems.
Financial Risk	Risk that could result in a negative impact to the agency(waste or loss of funds/assets).
Legal Risk	Risk associated with legal or regulatory actions and agency's capacity to consummate important transactions, enforce contractual agreements, or meet compliance and ethical requirements.
Legislative Risk	Risk that legislation could significantly alter the mission (funding, customer base, level of resources, services, and products) of the agency.
Operational Risk	Risk of direct or indirect loss or other negative effects to an entity due to inadequate or failed internal processes arising from people, systems, or from external events that impair those internal processes, people or systems. Operational risks are a broad risk category in part because a broad range of risks (e.g., legal, compliance and other risk types identified in this section) can have a direct impact on daily operations of an enterprise.
Political Risk	Risk that may arise due to actions taken by Congress, the Executive Branch or other key policy makers that could potentially impact business operations, the achievement of the agency's strategic and tactical objectives, or existing statutory and regulatory authorities. Examples include debt ceiling impasses, government closures, etc.

Risk Type	Risk Description
Reporting Risk	The risk associated with the accuracy and timeliness of information needed within the organization to support decision making and performance evaluation, as well as, outside the organization to meet standards, regulations, and stakeholder expectations. This is a subset of operational risk.
Reputational Risk	Risk that a failure to manage risk, external events, and external media or to fail to fulfill the agency's role (whether such failure is accurate or perceived) could diminish the stature, credibility or effectiveness of the agency. Reputational risk can arise either from actions taken by the agency or third party partners including service providers and agents. Reputational Risk can also arise from negative events in one of the other risk categories such as Legal and Compliance risks.
Strategic Risk	Risk that would prevent an area from accomplishing its objectives (meeting the mission).

1. Credit Risk

Although the government is often able to achieve these policy goals in a cost effective way using credit assistance, credit assistance exposes taxpayers to unique risks not be present in other forms of Federal assistance, such as repayment risk, prepayment risk, and market risk. Legislators and agencies must consider and account for these risks when determining if credit assistance is appropriate, as well as when designing and operating Federal credit programs.

The goal of risk management functions in the Federal credit context is to ensure the agency achieves policy outcomes at lowest cost to the taxpayer, and to identify, measure, monitor, and control risks that may reduce the agency's ability to achieve its objectives. Federal credit risk managers must also minimize risk subject to statutory and other program requirements. It is essential for Agencies to include programmatic requirements and objectives as a part of any credit risk presentation or discussion. This information is critical to performing appropriate cost benefit analyses that should be the basis of program decisions; as these risks are often deliberately taken to achieve a specific policy objective.

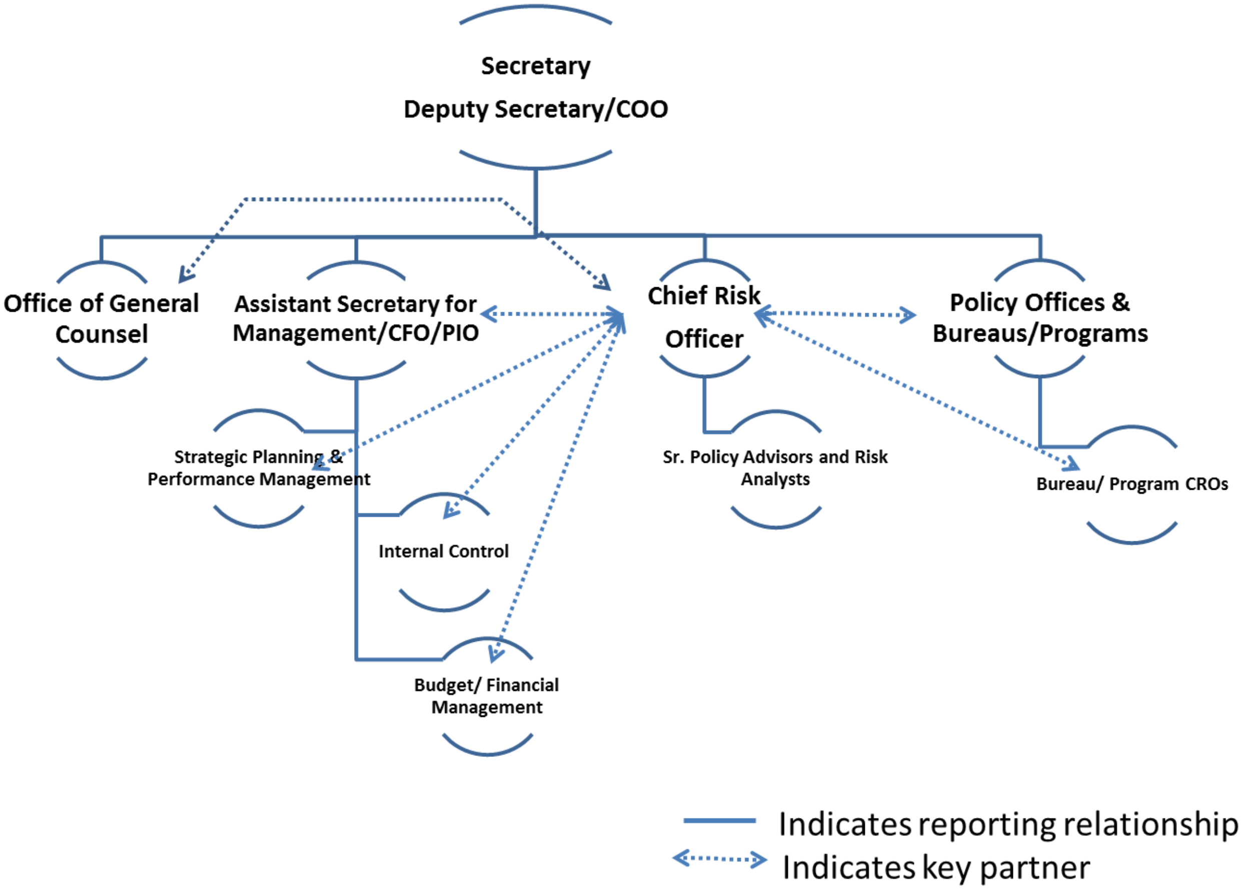
Additional challenges faced by Federal agencies in implementing credit programs are the increased administrative burden and operational risks associated with running credit programs compared with other forms of Federal assistance. Agencies require robust management and oversight structures to ensure progress towards policy goals, costs, and risks are measured and accounted for correctly, and that staff at all levels have the appropriate experience and expertise necessary to perform the range of duties involved in running a credit program.

Due to the unique challenges and risks faced by agencies in running Federal credit programs, OMB issued Circular No. A-129, "Policies for Federal Credit Programs and Non-Tax Receivables" which prescribes policies and procedures for justifying, designing, and managing Federal credit programs and for collecting non-tax receivables. It also sets standards for extending credit, managing lenders participating in Government guaranteed loan programs, servicing credit and non-tax receivables, and collecting Program Reviews, credit risk oversight structures, dashboards, pipeline reports and watch lists specific to credit that Agencies can incorporate into their ERM processes.

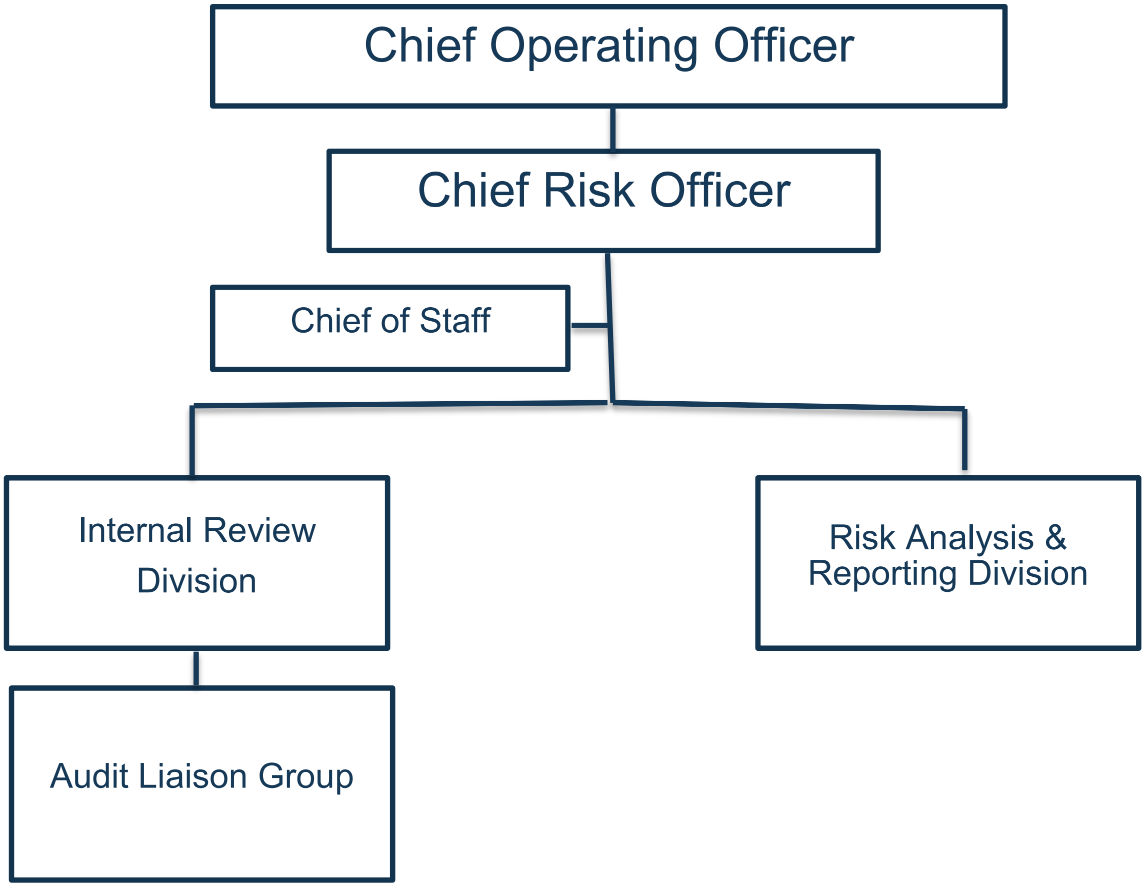
B. ERM Governance/ Culture/ Framework

1. Organization Charts

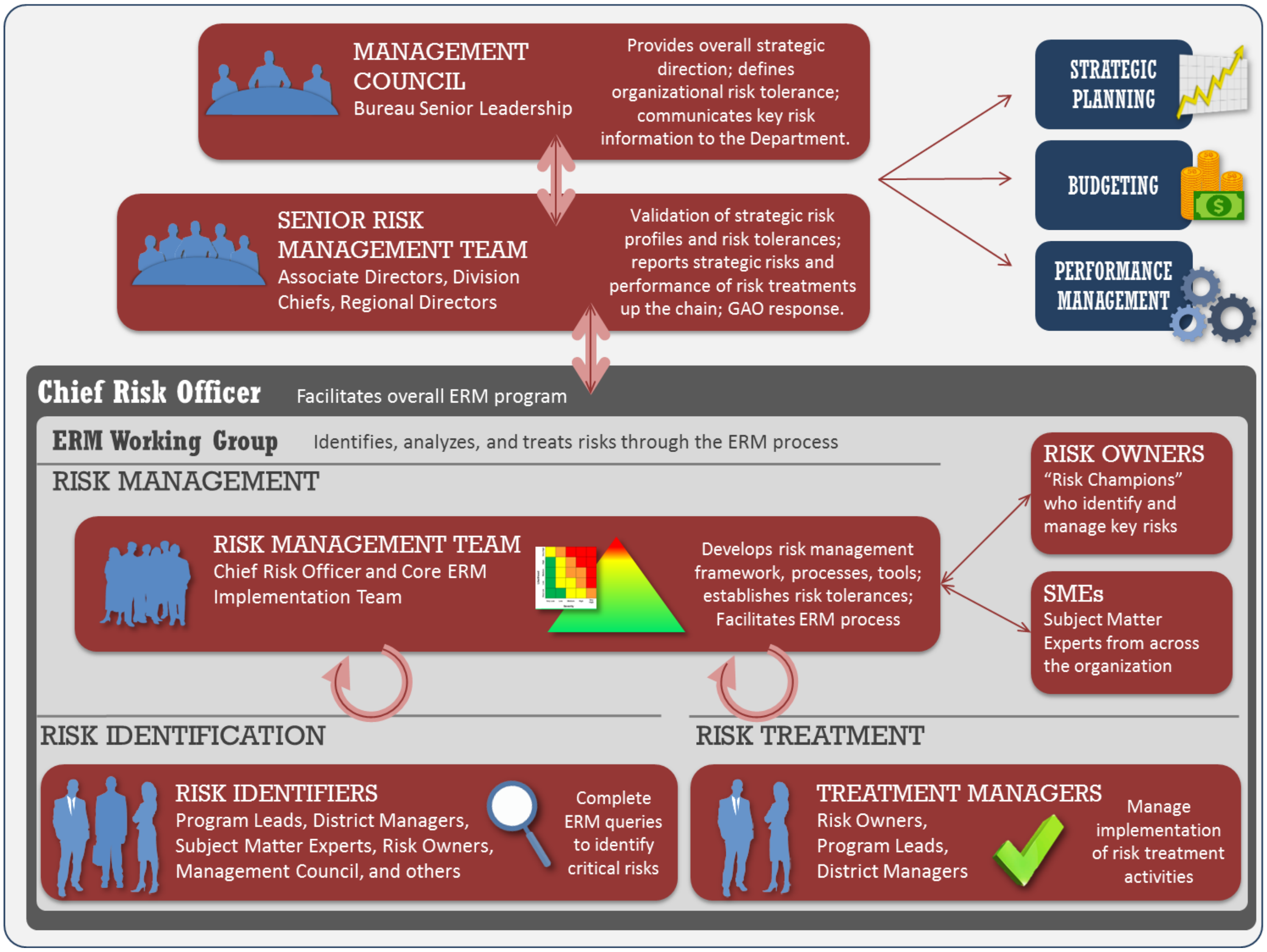
a. Relational Organization Chart in Agency with CRO Function at Senior Level (Example)


Secretary
Deputy Secretary/COO
Office of General Counsel
Assistant Secretary for Management/CFO/PIO
Chief Risk Officer
Policy Offices & Bureaus/Programs
Strategic Planning & Performance Management
Internal Control
Budget/ Financial Management
Sr. Policy Advisors and Risk Analysts
Bureau/ Program CROs
Indicates reporting relationship
Indicates key partner

b. Relational Organization Chart in Bureau with CRO Function at Senior Level (Example)



c. Relational Organization Chart in Bureau with CRO Function Embedded (Example)



MANAGEMENT COUNCIL
Bureau Senior Leadership

Provides overall strategic direction; defines organizational risk tolerance; communicates key risk information to the Department.

SENIOR RISK MANAGEMENT TEAM
Associate Directors, Division Chiefs, Regional Directors

Validation of strategic risk profiles and risk tolerances; reports strategic risks and performance of risk treatments up the chain; GAO response.

STRATEGIC PLANNING

BUDGETING

PERFORMANCE MANAGEMENT

Chief Risk Officer — Facilitates overall ERM program

ERM Working Group — Identifies, analyzes, and treats risks through the ERM process

RISK MANAGEMENT

RISK MANAGEMENT TEAM
Chief Risk Officer and Core ERM Implementation Team

Develops risk management framework, processes, tools; establishes risk tolerances; Facilitates ERM process

RISK OWNERS
"Risk Champions" who identify and manage key risks

SMEs
Subject Matter Experts from across the organization

RISK IDENTIFICATION

RISK IDENTIFIERS
Program Leads, District Managers, Subject Matter Experts, Risk Owners, Management Council, and others

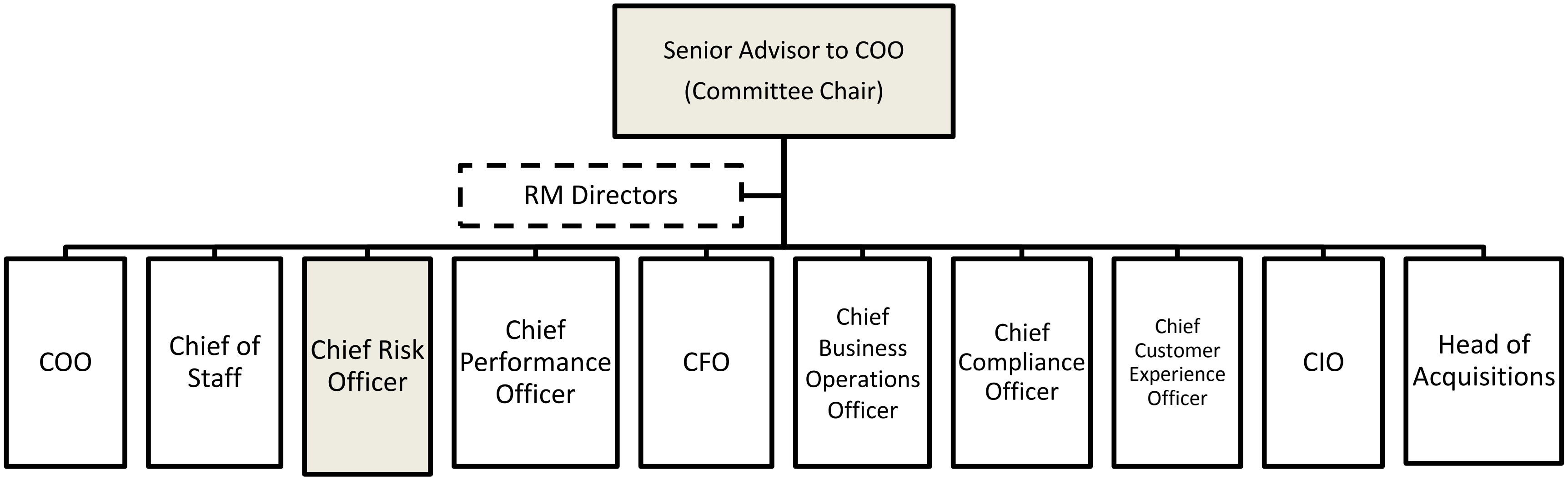
Complete ERM queries to identify critical risks

RISK TREATMENT

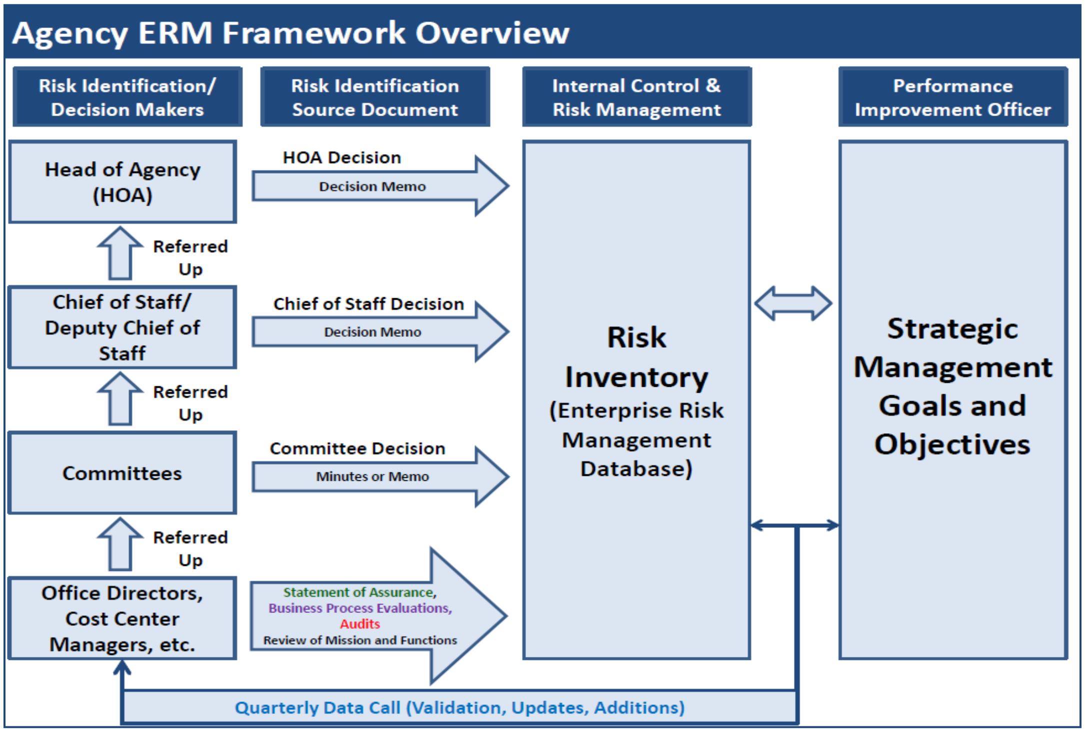
TREATMENT MANAGERS
Risk Owners, Program Leads, District Managers

Manage implementation of risk treatment activities

d. Risk Management Committee (Example)



e. Relational Organization Chart in Agency with No Formal CRO (Example)



Agency ERM Framework Overview

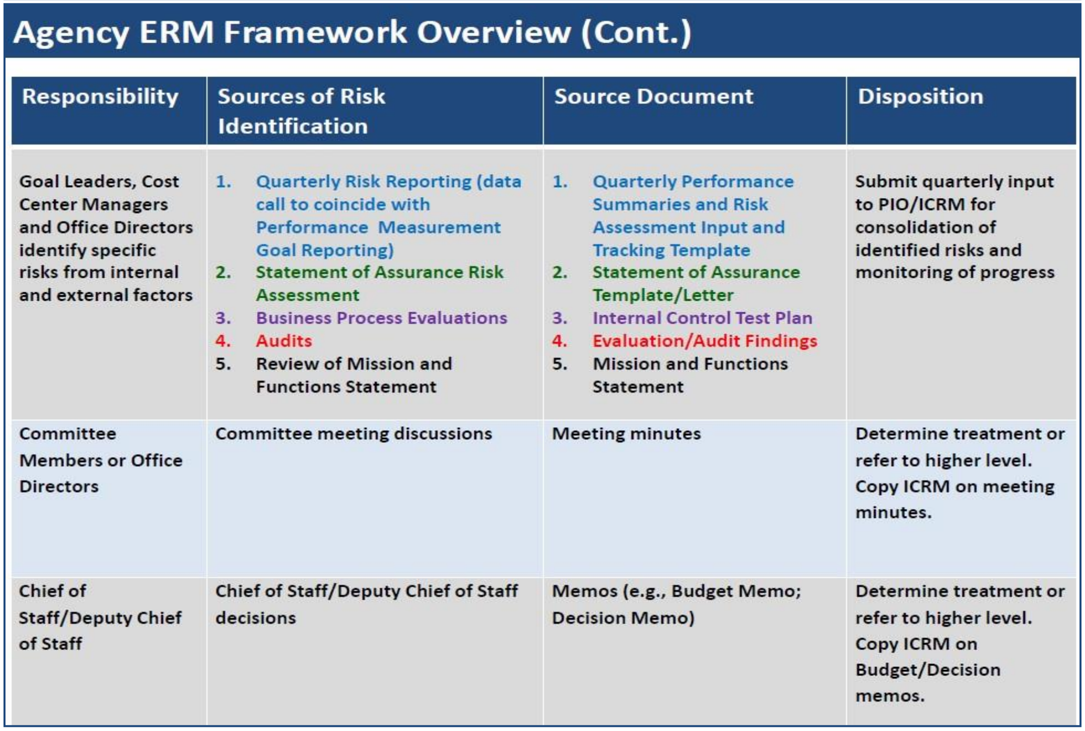
Risk Identification/ Decision Makers

Risk Identification Source Document

Internal Control & Risk Management

Performance Improvement Officer

Head of Agency (HOA)
HOA Decision
Decision Memo
Referred Up
Chief of Staff/ Deputy Chief of Staff
Chief of Staff Decision
Decision Memo
Referred Up
Committees
Committee Decision
Minutes or Memo
Referred Up
Office Directors, Cost Center Managers, etc.
Statement of Assurance,
Business Process Evaluations,
Audits
Review of Mission and Functions
Risk Inventory (Enterprise Risk Management Database)
Strategic Management Goals and Objectives
Quarterly Data Call (Validation, Updates, Additions)



Agency ERM Framework Overview (Cont.)

Responsibility	Sources of Risk Identification	Source Document	Disposition
Goal Leaders, Cost Center Managers and Office Directors identify specific risks from internal and external factors	1. Quarterly Risk Reporting (data call to coincide with Performance Measurement Goal Reporting) 2. Statement of Assurance Risk Assessment 3. Business Process Evaluations 4. Audits 5. Review of Mission and Functions Statement	1. Quarterly Performance Summaries and Risk Assessment Input and Tracking Template 2. Statement of Assurance Template/Letter 3. Internal Control Test Plan 4. Evaluation/Audit Findings 5. Mission and Functions Statement	Submit quarterly input to PIO/ICRM for consolidation of identified risks and monitoring of progress
Committee Members or Office Directors	Committee meeting discussions	Meeting minutes	Determine treatment or refer to higher level. Copy ICRM on meeting minutes.
Chief of Staff/Deputy Chief of Staff	Chief of Staff/Deputy Chief of Staff decisions	Memos (e.g., Budget Memo; Decision Memo)	Determine treatment or refer to higher level. Copy ICRM on Budget/Decision memos.

f. Relational Organization Chart in Agency with No Formal CRO (Example)

Role	Responsibilities
Standing Management Committees, for example: • Executive Management Council (EMC) • Risk Management Council (RMC) • Senior Assessment Team (SAT) • Audit Committee	• Responsible for identifying risks associated with their respective subject areas (i.e., budget and finance; human resources; IT; strategic planning, performance planning, and strategic review processes) • Solicit, track, analyze, monitor, and report risks identified during committee meetings, presented by the Office Directors/Goal Leaders/Cost Center Managers, to the Executive Management Council (EMC), other committees, and other internal and external sources • Respective committee chairs work with the Chief Operating Officer, Chief of Staff and Director of Internal Control and Risk Management (ICRM) to consolidate, prioritize, and present agency-wide risks to the Head of the Agency
Chief Operating Officer (COO)	• Identify and coordinate actions that improve results, enhance efficiency, manage risks, and reduce waste • Incorporate risk discussions in the strategic planning and performance management processes • Track risks • Facilitates discussions on risk prioritization for the agency • Analyzes the impact of specific risk to the agency • Coordinates the development of risk mitigation plans where and if applicable • Works with the EMC, ICRM, PIO, and Committee chairs and members to present risks to the Head of the Agency
Chief of Staff and Deputy Chief of Staff	• Ensures that risks, as identified in decision memos, are communicated to the Head of the Agency, to the EMC/appropriate committees, the COO, and ICRM
Internal Control and Risk Management Division (ICRM)	• Provides guidance to help the Agency develop a common vision, definition, and strategy for managing risk • Facilitates the development of a common language and clarifies terminology to enable constructive discussions • Provides guidance to establish and implement an ERM framework that facilitates the use of the risk cycle approach • Works with the CAO, CFO, CIO, COO, GC, PIO, and Office of Budget to track and report organizational risks • Monitor and validate risks identified within the ERM Database
Performance Improvement Officer (PIO)	• Promotes the application and execution of risk management practices in the strategic planning, performance planning and reporting, and strategic review processes
Office of Budget	• Incorporates risk management practices in the budget formulation and execution processes
Office Directors/Goal Leaders/Cost Center Managers	• For their areas of responsibilities: ○ Conduct risk analysis: ▪ Description of risk

Role	Responsibilities
	▪ Annual Performance Plan Objective (if applicable) ▪ Related Project or Function ▪ Risk Treatment Category and Description ▪ Resources Required and Cost ▪ Probability of Occurrence of Identified Risk ▪ Impact of Identified Risk ▪ Type of Risk • Consult with ICRM as needed • Document and validate risks using the Enterprise Risk Management Database • Present risk analysis to the appropriate committee(s)

2. Position Descriptions

a. Chief Risk Officer (Financial Agency) Position Description (Example)

Chief Risk Officer (CRO)

Introduction

The incumbent of this position serves as the Chief Risk Officer (CRO), Office of Risk Management, [AGENCY]. The Office of Risk Management (ORM) serves as an agency-wide mechanism ensuring that (a) risks across the [AGENCY] are considered in aggregate; (b) risk management activities across the [AGENCY] are coordinated so that similar risks are considered in a similar fashion; and (c) there is an independent viewpoint on major risk related decisions and assumptions across the [AGENCY].

Risk management functions in operations, credit programs, other financial exposures, and activities within the government are envisioned to act as a check-and-balance to those that make operational, credit and market-risk decisions, and to advise management concerning actual and potential risks, particularly changes in risk levels in real time. While the objective is not to second-guess decisions after they have been made, review of failures or other issues should be undertaken to further improve processes, as appropriate. It should be clear from these potential roles that the risk management function is intended to partner with existing program staff and leadership to foster a culture of risk management within [AGENCY] and a comprehensive understanding of potential risks.

The CRO will provide executive-level management, leadership, direction and oversight to the ORM and expertise to the [AGENCY] by identifying and advising on mitigation efforts regarding the most significant risks facing the [AGENCY] including operations, credit programs, financial exposures and activities including credit, market, liquidity, operational, governance, and reputational risks. The variety and technical complexity of issues and problems require (a) an in-depth understanding of Federal credit programs and other programs that present financial exposure and other risks to the U.S. government, (b) mature judgment, and (c) thoughtful and constructive analysis. The work requires flexibility in developing solutions and executing actions, while maintaining adherence to law, regulation, and rule. The work requires a constructive approach to problem solving, which includes taking initiative in (a) the identification of needs and potential problems, (b) finding potential solutions, and (c) supporting active and well-informed management and supervisory participation.

Assignments are complex, sensitive, and wide reaching in scope.

Duties and Responsibilities

- The CRO has responsibility for forecasting the [AGENCY]'s risk management needs, and independently oversees the development and implementation of an integrated risk management framework for the [AGENCY].
- Works closely with senior [AGENCY] and other Administration officials to recommend and promote best practices in risk management and ensures that all such analyses are thorough, accurate, and authoritative. Makes recommendations concerning which options are most appropriate.
- Compares existing [AGENCY] program-level risk-management practices against public and private sector "best practices" to propose and implement improvements, as needed. Develops plan to further formalize risk management practices across the [AGENCY]. Reviews existing program level risk reporting and works to enhance where necessary.
- Promotes a best-practice risk-management culture at the [AGENCY].
- Formulates and plans strategic and operational direction and expertise to the Office of Risk

Chief Risk Officer (CRO)

Management. Hires and supervises the Office's professional and support staff, and promotes the career development of each member of the staff. Provides both administrative and substantive direction, guidance, and encouragement to the staff, formulates performance expectations for each staff member, provides performance feedback, and prepares annual staff evaluations.

- Provides executive leadership and overall direction to the Office of Risk Management's administrative support functions. This includes the programs of strategic planning, human capital management, budget, accounting and financial systems, organizational and management analysis, program performance analysis, and administrative services.
- Leads multiple projects simultaneously and directs and supervises the crafting of briefing materials, issue papers, memoranda, reports, and studies. Develops [AGENCY]-wide risk monitoring reports, including risk assessments.
- Provides senior [AGENCY] officials and other Administration officials with quantitatively and qualitatively rigorous analyses on key risks including credit, market, liquidity, operational, governance, and reputational risks.
- Formulates an integrated risk management framework with emphasis on analyzing and developing policy, mitigation of risks, determination, measurement and monitoring of risk appetite, and understanding the interrelationships of various types of risk.
- Plans, develops, recommends, coordinates, and implements financial management policies and strategies, as well as designs management techniques to achieve risk-management goals.
- Represents [AGENCY] in departmental, interdepartmental, Congressional, and private sector meetings and conferences. Establishes and maintains close and continuing contact and effective liaison with [AGENCY] policy offices and bureaus, congressional and agency staffs, and high-ranking representatives of the financial community, consumer and community organizations, and other government agencies, and government officials.
- Collaborates with the other offices within the [AGENCY] in the development of policies, proposals, reports, briefings, and other assignments, and, as appropriate, in administrative and staffing matters.

Supervision and Guidance Received

The incumbent reports directly to the Deputy Secretary of the [AGENCY] who (a) provides policy direction and guidance; (b) defines the role of the incumbent; (c) delegates sufficient authority to allow fulfillment of that role; (d) communicates relevant policy information; and (e) evaluates the incumbent's performance in terms of results achieved, effective leadership of subordinates, and contribution to the overall management and administration of the [AGENCY]. Within the overall goals established by the Deputy Secretary, the incumbent has broad discretion and is responsible for selecting and defining both short-term and longer term program objectives.

Subject areas are broad and complex and accomplishing the duties of the position requires considerable ingenuity and originality, as well as considerable knowledge of financial   institutions and markets, economic theory, and the legal and regulatory environment. Results of work are considered to be professionally authoritative and are normally accepted without significant change.

The incumbent is expected to initiate analytical work and policy analysis and completed work is reviewed by the Deputy Secretary to assure conformance to broad [AGENCY] policies, and to ascertain that the broad policy objectives of the [AGENCY] are carried out.

Chief Risk Officer (CRO)

Job Competencies (The full range of competencies for the occupational series is provided for information and development purposes.)

- Executive knowledge of risk management best practices in the public and/or private sector.
- Demonstrated ability to resolve complex risk-management issues and create financial analysis documents on an executive level.
- Executive knowledge of complex risk-related financial analysis techniques, applications, records, and reporting.
- Ability to communicate effectively, brief senior officials regarding options and recommendations, and inspire confidence in those recommendations and decisions.
- Ability to quickly develop a strong understanding and knowledge of the major operational functions of [AGENCY], including the organization's mission and function, programs, policies, procedures, rules, and regulations.
- Ability to quickly identify and analyze problems, distinguish between relevant and irrelevant information to perform logical risk-related financial analyses, and propose solutions to individual and organizational problems.
- Demonstrates the ability to lead, manage, and facilitate change; demonstrates the vision to define and effectively manage strategies, change structures, and change processes necessary to address program priorities of the [AGENCY].
- Ability to develop steps, schedules, and assignments to meet strategic goals and targets; manage implementation of projects and initiatives; anticipate and adjust for problems; measure outcomes; and evaluate and report results.
- Ability to instill trust and confidence; create a culture that fosters high standards of ethics; behave in a fair and ethical manner toward others, and demonstrate a sense of responsibility and commitment to public service.
- Ability to respond appropriately to the needs, feelings, and capabilities of different people in different situations; to be tactful, compassionate, and sensitive; and to treat others with respect.
- Ability to facilitate collaboration, cooperation, peer support, open dialogue, shared responsibility and shared credit among work group members; develop leadership in others through coaching, mentoring, rewarding, and guiding.
- Ability to plan and develop a workforce prepared to meet current and future [AGENCY] risk management needs.
- Ability to apply Equal Employment Opportunity and Merit System principles to ensure staff members are appropriately selected, developed, utilized, praised, and rewarded.

b. Chief Risk Officer (Financial Agency) Position Description (Example)

Chief Risk Officer (CRO)

Introduction

This position is located in [Office], [Agency], Enterprise Performance Management Services (EPMS). EPMS is responsible for providing best service in business service for project management oversight and strategic planning, contract management, risk management, internal review and internal audit tracking, as well as operational performance analysis and reporting.

The incumbent of this position serves as the Chief Risk Officer (CRO) for [Agency] and reports to the General Manager for EPMS. Responsibilities include implementing a coordinated approach for identifying, assessing, monitoring, and reporting on risk throughout the organization, managing the internal audit resolution process for [Agency], and developing an internal review capability to evaluate the programs, policies, procedures, systems, and controls at [Agency], its contractors, and program partners. The incumbent serves as the agency's risk management expert and internal consultant and change agent with a strategic business focus. Generates creative solutions to issues and concerns that are in keeping with the overall agency mission, vision, and goals.

Major Duties

- The CRO is responsible for the management and oversight of the Enterprise Risk Management Group, which includes the Internal Review and the Risk Analysis and Reporting Divisions. The incumbent directs the activities of those organizations in an effort to ensure that they meet their objectives as established.
- The incumbent fosters close ties with the Government Accountability Office (GAO), Office of Inspector General (OIG), and other agencies or offices both outside and inside the agency, in an effort to facilitate their activities, coordinate efforts, and ensure that all significant matters receive the appropriate attention of agency Management.
- The CRO provides expertise, leadership and overall strategic guidance to the General Manager of EPMS, the Chief Operating Officer (COO) and members of the agency's Management Council, in areas such as risk assessment, risk management, project funding oversight, internal reviews, compliance with Federal regulations and evaluation of internal controls. The incumbent will serve as a principal advisor and expert to the General Manager of EPMS, and will be responsible for providing regular reports to the Chief Operating Officer along with conducting special reviews, risk assessments, or other special projects at her/his request, which includes accessing sensitive data.
- Responsible for implementing an ERM framework and strategy for the organization. Coordinates an annual high-level risk assessment at the agency and helps to facilitate an integrated and enterprise-wide view of risk, risk tolerances and risk mitigation efforts. Oversees the development of improved methodologies for identifying, quantifying, and reporting on risks affecting the organization and the organization's overall risk profile.
- Serves as an internal consultant to the General Manager for EPMS and the COO. Develops creative solutions to unique and systemic problems and acts as a change agent through the implementation of solutions, recommending systems and structures needed to support changes, preparing staff to manage change, and anticipating and dealing effectively with resistance to change.

Supervision Received

The incumbent reports directly to the General Manager of EPMS who provides broad policy guidance and direction. The incumbent is allowed a wide degree of latitude in making independent decisions with regard to planning and managing projects and major activities of the organization. Work performance is evaluated in terms of overall effectiveness and accomplishment of goals and objectives established by

Chief Risk Officer (CRO)
the General Manager for EPMS.
Supervision Exercised
The incumbent will be required to independently develop recommendations for other EPMS staff to implement.

c. *Director, Risk Analysis and Reporting (Example)*

Director, Risk Analysis and Reporting

Introduction

This position is located in the [AGENCY], [PROGRAM], Enterprise Performance Management Services (EPMS), Enterprise Risk Management Group (ERMG). EPMS is responsible for providing best in business service for project management, oversight and strategic planning, contract management, enterprise-wide risk management, internal review and tracking of internal audits, and operational performance analysis and reporting.

Major Duties

- Directs the implementation of agency's Enterprise Risk Management (ERM) Program.
- Implements strategies and provides guidance for improving risk management practices across the organization.
- Manages staff of Risk/Data Analysts, providing direction on various risk management and data analyses efforts including: activities supporting the implementation of the agency's ERM Program; conduct of, or involvement with risk assessments, risk training or the development of risk management strategies across the agency; and the development & maintenance of ERMG's Risk Tracking System (RTS), other data initiatives and risk analyses supporting the goals of the agency and ERMG.
- Directs and develops plans for project teams or other groups to complete projects, studies, and risk assessments.
- Analyzes and evaluates on a quantitative and qualitative basis the effectiveness of line program operations in meeting established goals and objectives and identifying/managing risks.
- Provides day to day oversight and technical direction to contractors supporting the agency's ERM Program and other ERMG initiatives.
- Develops, analyzes, and evaluates new or modified program and management policies, regulations, goals, or objectives.
- Develops procedures and systems for assessing the effectiveness of programs and management processes.

Factor Levels

FACTOR 1 KNOWLEDGE REQUIRED Level 1-8 1550 points

- Knowledge at a level to serve as an expert in the application of a wide range of qualitative and quantitative methods for the assessment and improvement of program effectiveness or the improvement of complex management processes and systems.
- Knowledge of a comprehensive range of administrative laws, policies, regulations, and precedents applicable to the administration of one or more programs.
- Knowledge of program goals and objectives, the sequence and timing of key program events and milestones, and methods of evaluating the worth of program accomplishments.
- Knowledge of relationships with other programs and key administrative support functions within the agency or other agencies.
- Knowledge of advanced risk management and analytical practices, standards, and procedures.
- Skill to plan, organize, and direct team study work and to negotiate effectively with management to accept and implement recommendations, where the proposals involve substantial agency resources, require extensive changes in established procedures, or may be in conflict with the desires of the activity studied.

Director, Risk Analysis and Reporting

FACTOR 2 SUPERVISORY CONTROLS Level 2-5 650 points

The employee is subject only to administrative and policy direction concerning overall project priorities and objectives. The employee is typically delegated complete responsibility and authority to plan, schedule, and carry out major projects concerned with the analysis and evaluation of programs and organizational effectiveness. Analyses, evaluations, and recommendations developed by the employee are normally reviewed by management officials only for potential influence on broad agency policy objectives and program goals.

FACTOR 3 GUIDELINES Level 3-5 650 points

Guidelines consist of basic administrative policy statements concerning the issue or problem being studied. The employee uses judgment and discretion in interpreting and revising existing policy/regulatory guidance for use by others. Some employees review proposed regulations that would significantly change the basic character of programs, the way the agency conducts its business with the public or with the private sector. Develops study formats for use by others on a project team or at subordinate echelons in the organization.

FACTOR 4 COMPLEXITY Level 4-5 325 points

The work consists of complex projects and studies that require extensive analysis of interrelated issues of effectiveness, efficiency, and productivity of substantive mission-oriented programs. Decisions about how to proceed in planning, organizing and conducting studies are complicated by conflicting program goals and objectives. Options, recommendations, and conclusions developed by the employee take into account and give appropriate weight to uncertainties about the data and other variables that affect long-range program performance.

FACTOR 5 SCOPE AND EFFECT Level 5-5 325 points

The purpose of the work is to analyze and evaluate major management and program aspects of substantive, mission-oriented programs. The work involves identifying and developing ways to resolve problems or cope with issues that directly affect the accomplishment of principal program goals and objectives. Work products are complete decision packages and staff studies, and typically contain findings and recommendations of major significance that serve as the basis for new administrative systems, legislation, regulations, or programs.

FACTORS 6&7 PERSONAL CONTACTS AND
PURPOSE OF CONTACTS Level 3c 180 points

Contacts are with persons outside EPMS and with high-level program officials in a moderately structured setting. The purpose of contacts is to influence managers or other officials to accept and implement findings and recommendations on organizational improvement or program effectiveness. The employee may encounter resistance due to organizational conflict, competing objectives, or resource problems.

FACTOR 8 PHYSICAL DEMANDS Level 8-1 5 points

No unusual physical exertion is required.

Director, Risk Analysis and Reporting

FACTOR 9 WORK ENVIRONMENT Level 9-1 5 points

The work is performed in an office setting.

Unique Position Requirements

- Develops and maintains good working relationships with program, Departmental and external management and staff, represents ERMG and/or EPMS at Departmental meetings, and participates in interagency or Departmental work groups.
- Develops, conducts, and documents assessments of internal agency processes, which includes accessing sensitive data, designed to identify areas of operational risk and makes recommendations for risk management, monitoring strategies, and enhancements to processing efficiency.
- Facilitates Risk Management activities, policies, practices and standards and disseminates relevant information to agency and Departmental management and staff.
- Develops training programs, and provides training to agency and Departmental management and staff, on agency's Risk Management Strategy and Framework.
- Assists and advises agency managers in responding to audit findings, which include sensitive data that identify areas of risk /internal control weaknesses to agency programs.
- Monitors the execution of corrective action plans implemented to address audit/risk recommendations and reports on their effectiveness and value.
- Develops analytical and comparative risk reports for monthly/quarterly/annual statistical reporting.
- Analyzes various risk data and information applicable to agency's ERM Framework and helps to institutionalize and encourage behavior consistent with that framework.
- Designs, develops, and documents qualitative and quantitative statistics and tolerance levels in order to proactively monitor potential high risk issues.
- Designs, develops, and documents risk-related scorecards and other risk management tools in support of agency's ERM Framework.
- Presents and communicates results of analytical activities and findings in a manner consistent with target audience (technical/financial/operational).
- Interprets work requests and applies appropriate business logic.
- Oversees Risk Analysts, Data Analysts, and Management Program Analysts and directs them in interpretation and application processes.
- Provides management with timely communication on project status and needs; updates timesheets/project status reports as necessary/requested.
- Assumes responsibility for the accuracy and quality of work performed. Takes ownership of all assigned projects.
- Consults on agency policies and procedures.

d. Senior Policy Advisor (Financial Agency) Position Description (OFFICE OF RISK MANAGEMENT) (Example)

Senior Policy Advisor

Introduction

The purpose of this position is to serve as a Senior Policy Advisor, Office of Risk Management, [AGENCY]. The incumbent will advise the Chief Risk Officer, the Deputy Secretary, and the Secretary of the [AGENCY] on policies relating to the risk management of the operations and programs of [AGENCY] and throughout the Federal government. The incumbent will also assist in the development and implementation of policy that directly impacts the risk management of programs.

This position will serve as an expert specialist on a wide range of risk management matters, and provide assistance in identifying and advising on mitigation efforts regarding the most significant risks facing [AGENCY] and the Federal government. This position will involve handling difficult and responsible assignments, including research and analysis of current law and legislative proposals involving highly complex financial, legal, and budgetary issues. The position will plan and prepare reports that include recommendations and conclusions on which [AGENCY] policy may be developed.

Major Duties and Responsibilities

Under the general direction of the Chief Risk Officer, the Senior Policy Advisor shall:

- Plan, develop, recommend, coordinate, and implement risk management policies and strategies, as well as design management techniques to achieve risk management goals.
- Compare existing [AGENCY] program-level risk management practices against public and private sector (best practices) to propose and implement improvements as needed.
- Review existing program-level risk reporting, and work to enhance risk reporting where necessary.
- Develop [AGENCY]-wide risk monitoring reports, including detailed risk assessments.
- Provide technical support and analyses on credit, market, and liquidity issues, as well as on non-financial risks, such as operational, governance, and reputational risks.
- Summarize findings and research in written products of various types, including tables, charts, short summaries, as well as longer analytical policy memos and reports.
- Conduct complex and authoritative research relating to proposals that affect the financial exposure of [AGENCY] programs.
- Develop, produce and prepare policy statements, written materials, including briefing or issue papers, and memoranda for the Chief Risk Officer and other senior [AGENCY] officials, including the Secretary, and for White House officials, including for the purpose of meetings, speeches, interviews, and testimony.
- Prepare responses to Congressional, press or other public inquiries.
- Coordinate with senior officials at the Office of Management and Budget and other Federal agencies to effectively assess and mitigate risks, and ensure that applicable OMB guidelines, directives, and standards are effectively met by [AGENCY] programs.
- Maintain strong working relationships and ongoing lines of communication with officers and other staff members.
- Promote a strong culture of risk management.
- Provide guidance to junior-level staff as needed.
- Perform other duties as assigned.

Factor Levels

FACTOR 1: KNOWLEDGE REQUIRED BY THE POSITION (1-8 1550 Points)

Senior Policy Advisor

- Expert knowledge of risk management best practices in the public and/or private sector.
- Expertise in analyzing complex risk management issues affecting Federal credit, insurance, and other programs.
- Ability to analyze and convey detailed financial information presented in the U.S. budget.
- Expert knowledge of budgetary and legislative processes and practices relating to Federal credit programs, as well as a deep understanding of the Federal Credit Reform Act of 1990 and related law.
- Expert knowledge of risk management directives and policies set forth by [AGENCY] and OMB.
- Knowledge of complex risk-related financial analysis techniques, applications, records, and reporting.
- Skill in quickly gathering information about a new, complex topic, and summarizing orally and in writing information gathered.
- Ability to communicate effectively with senior [AGENCY] officials and provide recommendations to the Chief Risk Officer and the Deputy Secretary.

FACTOR 2: SUPERVISORY CONTROLS (2-5 650 Points)
Reports to the Chief Risk Officer, who provides limited supervision. The Senior Policy Advisor has complete authority to plan and carry out the work. Often, assignments require originality and ingenuity to determine how to approach any particular task in light of the overall goals. Work is reviewed by evaluating work product for potential influence on broad agency policy objectives.

The incumbent is viewed as a technical authority.

FACTOR 3: GUIDELINES (3-5 650 Points)
The Senior Policy Advisor uses judgment in interpreting and adapting guidelines such as administrative policy statements, which may include reference to pertinent legislative history.

The incumbent uses initiative and resourcefulness in deviating from traditional methods or in developing new methods, criteria, or proposed new approaches. The incumbent is recognized as an expert in the development and interpretation of guidance for the Office of Risk Management.

FACTOR 4: COMPLEXITY (4-6 450 Points)
Assignments vary in complexity due to the variety of tasks performed. Generally, the Senior Policy Advisor is required to quickly and independently perform analysis and develop recommendations that often require a high degree of complexity. The incumbent must effectively communicate, orally and in writing, summary findings on a range of risk management issues.

The incumbent plans, organizes, and carries out analysis of the economic, financial, and policy implications of matters relevant to the Office of Risk Management. Studies require input and assistance from other analysts and subject-matter specialists. The incumbent must determine the nature of issues and problems to be studied, which involves extreme difficulty when planning, organizing, and determining the scope and depth of the study. The nature and scope of the issues are largely undefined.

FACTOR 5: SCOPE AND EFFECT (5-6 450 Points)
The purpose of this position is to support the goal of improving risk management practices and

Senior Policy Advisor

outcomes among operations and programs within [AGENCY] and throughout the Federal government. It involves providing the necessary analytical, evaluative, and communications skills to substantive mission-oriented programs of the Office of Risk Management. The scope of work assignments is unusually broad and often serve as a basis for new administrative systems, legislation, regulations, or programs.

FACTOR 6: PERSONAL CONTACTS (6-4 7-D 330 Total Points)
Contacts are with the personnel in [AGENCY], other Federal agencies, and representatives of business and non-profit organizations. Contacts also are high-ranking officials such as agency heads and congressional staff officials.

FACTOR 7: PURPOSE OF CONTACTS (Points combined with factor 6)
The purpose of this position is to make recommendations to the Chief Risk Officer and to justify or settle matters involving significant or controversial issues. Also, personal contacts are for the purpose of gathering information and gaining insight into issues related to the effective risk management of [AGENCY] operations and programs. The incumbent participates in meetings and discussions on these issues.

FACTOR 8: PHYSICAL DEMANDS (8-1 5 Points)
The work is generally sedentary, however, there may be some walking, standing, carrying of light items. No special physical demands are required to perform the work.

FACTOR 9: WORK ENVIRONMENT (9-1 5 Points)
Work is usually performed in an office setting.

Total Points = 4090

In accordance with the implementation of the Homeland Security Presidential Directive 12 (HSPD 12) - Policy for a Common Identification Standard for Federal Employees and Contractors all employees must meet the following requirements:
(1) Be eligible for a Personal Identity Verification (PIV) Credential;
(2) Have a successfully adjudicated NACI or equivalent background investigation; and
(3) Maintain PIV credential eligibility during their service with the [AGENCY].

e. Senior Risk Analyst Position Description (Example)

Senior Risk Analyst

Introduction

This position is located in the [Agency], [Program], Enterprise Performance Management Services (EPMS), Enterprise Risk Management Group (ERMG). EPMS is responsible for providing best in business service for project management, oversight and strategic planning, contract management, enterprise-wide risk management, internal review and tracking of internal audits, and operational performance analysis and reporting.

Major Duties and Responsibilities

- Directs and develops plans for project teams or other groups to complete projects, studies, and risk assessments.
- Analyzes and evaluates on a quantitative and qualitative basis the effectiveness of line program operations in meeting established goals and objectives and identifying and managing risks.
- Evaluates and advises on organization, methods, and procedures.
- Analyzes management information requirements.
- Develops, analyzes, and evaluates new or modified program and management policies, regulations, goals, or objectives.
- Develops procedures and systems for assessing the effectiveness of programs and management processes.

Factor Levels

FACTOR 1 KNOWLEDGE REQUIRED Level 1-8 1550 points

- Knowledge at a level to serve as an expert in the application of a wide range of qualitative and quantitative methods for the assessment and improvement of program effectiveness or the improvement of complex management processes and systems.
- Knowledge of a comprehensive range of administrative laws, policies, regulations, and precedents applicable to the administration of one or more programs.
- Knowledge of program goals and objectives, the sequence and timing of key program events and milestones, and methods of evaluating the worth of program accomplishments.
- Knowledge of relationships with other programs and key administrative support functions within the program or other agencies.
- Skill to plan, organize, and direct team study work and to negotiate effectively with management to accept and implement recommendations, where the proposals involve substantial program resources, require extensive changes in established procedures, or may be in conflict with the desires of the activity studied.

FACTOR 2 SUPERVISORY CONTROLS Level 2-5 650 points

The employee is subject only to administrative and policy direction concerning overall project priorities and objectives. The employee is typically delegated complete responsibility and authority to plan, schedule, and carry out major projects concerned with the analysis and evaluation of programs and organizational effectiveness. Analyses, evaluations, and recommendations developed by the employee are normally reviewed by management officials only for potential influence on broad agency policy objectives and program goals.

FACTOR 3 GUIDELINES Level 3-5 650 points

Senior Risk Analyst

Guidelines consist of basic administrative policy statements concerning the issue or problem being studied. The employee uses judgment and discretion in interpreting and revising existing policy/regulatory guidance for use by others. Some employees review proposed regulations that would significantly change the basic character of the program, the way it conducts its business with the public or with the private sector. Develops study formats for use by others on a project team or at subordinate echelons in the organization.

FACTOR 4 COMPLEXITY Level 4-5 325 points

The work consists of projects and studies that require analysis of interrelated issues of effectiveness, efficiency, and productivity of substantive mission-oriented programs. Decisions about how to proceed in planning, organizing and conducting studies are complicated by conflicting program goals and objectives. Options, recommendations, and conclusions developed by the employee take into account and give appropriate weight to uncertainties about the data and other variables that affect long-range program performance.

FACTOR 5 SCOPE AND EFFECT Level 5-5 325 points

The purpose of the work is to analyze and evaluate major management/program aspects of substantive, mission-oriented programs. The work involves identifying and developing ways to resolve problems or cope with issues that directly affect the accomplishment of principal program goals and objectives. Work products are complete decision packages and staff studies, and typically contain findings and recommendations of major significance that serve as the basis for new administrative systems, legislation, regulations, or programs.

FACTORS 6&7 PERSONAL CONTACTS AND
PURPOSE OF CONTACTS Level 3c 180 points

Contacts are with persons outside EPMS and with high-level program officials in a moderately structured setting. The purpose of contacts is to influence managers or other officials to accept and implement findings and recommendations on organizational improvement or program effectiveness. The employee may encounter resistance due to organizational conflict, competing objectives, or resource problems.

FACTOR 8 PHYSICAL DEMANDS Level 8-1 5 points

No unusual physical exertion is required.

FACTOR 9 WORK ENVIRONMENT Level 9-1 5 points

The work is performed in an office setting.

Unique Position Requirements

- Experience and expertise with risk management and/or data analysis applications.
- Assists in the development and maintenance of effective data mining and analysis capabilities to support risk management and internal review efforts throughout EPMS.
- Designs, develops, documents and implements processes and supporting analytical models to

Senior Risk Analyst
be used to evaluate risk and help ensure the accuracy and quality of data received from internal and external sources. • Provides data acquisition and application development support of risk-related projects including project design, data collection and transformation, source system data analysis, database design, analysis and presentation of results. • Analyzes and evaluates sensitive data within the agency's systems to identify any patterns, trends, or data anomalies. Interprets the data results in the context of laws and regulations governing the program. • Obtains, analyzes, and reviews various risk data and information applicable to the program's Enterprise-wide Risk Management Framework, which includes accessing sensitive data. • Produces analytical and comparative risk reports and utilizes various risk monitoring tools (i.e., scorecards, dashboards, etc.) to provide for regular (monthly/quarterly/annual) management reporting in support of the agency's Enterprise-wide Risk Management program. • Develops and maintains good working relationships with program, Departmental, and external management and staff, represents EPMS at Departmental meetings, and participates in interagency workgroups. • Presents and communicates results of analytical activities and findings in a manner consistent with target audience (technical/financial/operational). • Provides management with timely communication on project status and needs and updates timesheets and project status reports as necessary or as requested. • Assumes responsibility for the accuracy and quality of work performed. Takes ownership of all assigned projects. • Works cooperatively with independent contractors hired to assist with ERM efforts and supporting activities. Assists with the monitoring of contractors as directed. • Supervises, mentors, and trains junior staff as appropriate.

3. Risk Committee Charters

a. Risk Committee Charter – Agency with a CRO (Example)

This Charter describes the objectives, scope, functions, organizational structure, and operating procedures of [AGENCY] Risk Management Committee ("Risk Committee").

Objectives	The purpose of the Risk Committee is: (i) to monitor financial exposures and activities for various risks, including credit, market, liquidity, and operational risks; (ii) to receive updates on developments and discuss risks associated with financial exposures and activities with managers of these exposures and activities ("program managers"); and (iii) to review risk governance structure, including risk management practices and related issues.
Scope	The Risk Committee shall monitor and discuss the financial exposures and activities of the Agency for credit, market, liquidity, and operational risks.
Functions	The Risk Committee shall have the following functions: A. Monitor risk profiles and progress towards achieving policy goals for financial exposures and activities. B. Receive updates on and discuss risk management matters and risk profiles of financial exposures and activities. C. Advise program managers on the development and implementation of risk management guidelines, policies, and procedures with respect to financial exposures and activities. D. Discuss Agency-wide risk management practices. E. Help develop risk management best practices.
Organizational Structure	The Risk Committee will be comprised of the following Members: A. Deputy Head of Agency, who will serve as Co-Chair B. Chief Risk Officer, who will serve as Co-Chair C. All Program Under Secretaries and Assistant Secretaries
Meetings	The Risk Committee will endeavor to meet at least quarterly. Either Co-Chair will call meetings of the Risk Committee. A majority of the Members of the Risk Committee present at a meeting shall constitute a quorum. A. Minutes. The Office of Risk Management shall be responsible for preparing minutes of meetings. B. Agenda. The Office of Risk Management shall provide to Members the meeting agenda at least 48 hours in advance of the meeting. C. Attendance. Whenever appropriate, program managers and their supervisors will be invited to attend meetings of the Risk Committee at which their programs are being discussed or those where their expertise would be helpful to other programs.
Staffing	The Office of Risk Management shall support the Risk Committee at the direction of the Co-Chairs, and will perform administrative and other duties, including preparing minutes of meetings, as appropriate, in connection with the work of the Risk Committee.
Amendments	The Risk Committee will review this Charter at least annually, and may amend it in its discretion.
Effective Date	This Charter is effective immediately.

b. Risk Committee Charter – Agency without a CRO (Example)

Purpose	The purpose of the risk committee (the “Committee”) is to assist the AGENCY in fulfilling its oversight responsibilities with respect to the AGENCY’s enterprise risk management tolerance (including its risk appetite statement and risk management framework, including key strategic, reputational, regulatory, operational, and financial risks).
Authority	The Committee has authority to conduct or authorize reviews into any matters within its scope of responsibility. Specifically, it is empowered to: a) retain independent counsel, advisors or others to advise the Committee or assist in the conduct of its duties; b) seek any information it requires from employees, all of whom are directed to cooperate with the Committee's requests; c) meet with the officers, external advisors, auditors, or outside counsel, as necessary; and d) discharge any other duties or responsibilities delegated to it.
Composition	The Committee will consist of at least three and no more than five members of the AGENCY leadership. Committee members should have: a) expertise in risk governance and management, the risks the AGENCY faces, and methods for managing such risks; b) expertise in business activities (including finance), processes and risks similar to the size and scope of the AGENCY; c) expertise in risk committee functions; and d) the time, energy, and willingness to serve as active contributors.
Meetings	The Committee will meet periodically throughout the year at the call of the Chair as necessary to discharge its responsibilities, but not less than semiannually. A majority of the Committee members shall constitute a quorum (*i.e.*, two members constitute a quorum if the Committee consists of three members; three members constitute a quorum if the Committee consists of four or five members). Members may attend in person or via conference call or any other means by which all members may hear and respond to each other's statements contemporaneously. The Committee will invite members of management, contractors, or others to attend meetings and provide pertinent information, as necessary or appropriate. The Committee will hold private meetings and executive sessions as necessary. Meeting agendas will be prepared and provided in advance to the Committee, along with appropriate briefing materials. Minutes will be prepared.
Committee Duties and Responsibilities	AGENCY management has the duties and responsibilities of risk assessment, monitoring, and management. The Committee has an independent oversight role and, in fulfilling that role, relies on reviews and reports provided by AGENCY’s management. The Committee's duties and responsibilities shall include the following:

	a) review and discuss with AGENCY management, and provide guidance on: i. risk governance structure and framework; ii. risk appetite statement; iii. policies for enterprise risk assessment, monitoring, and management of, strategic, reputational, regulatory, operational, and financial risks; iv. periodic reports on selected risk topics as the Committee deems appropriate; and v. effectiveness of the system for monitoring the AGENCY's compliance with laws and regulations and the results of the AGENCY's management's investigation and follow-up (including disciplinary action) of any instances of noncompliance. b) receive reports from management on the metrics used to measure, monitor, and manage risks, and management's views on acceptable and appropriate levels of exposures; and c) receive reports on the status of internal and external reviews and audits and reports from internal and external reviewers and auditors. The Committee will report its activities and recommendations to the head of the AGENCY. Such reports will be made as necessary, but not less than annually.
Management Responsibilities	Management shall provide support sufficient to allow the Committee to carry out its duties and responsibilities and manage the schedule of the Committee such that all matters necessary to fulfilling the Committee's duties and responsibilities are properly and timely brought before it.

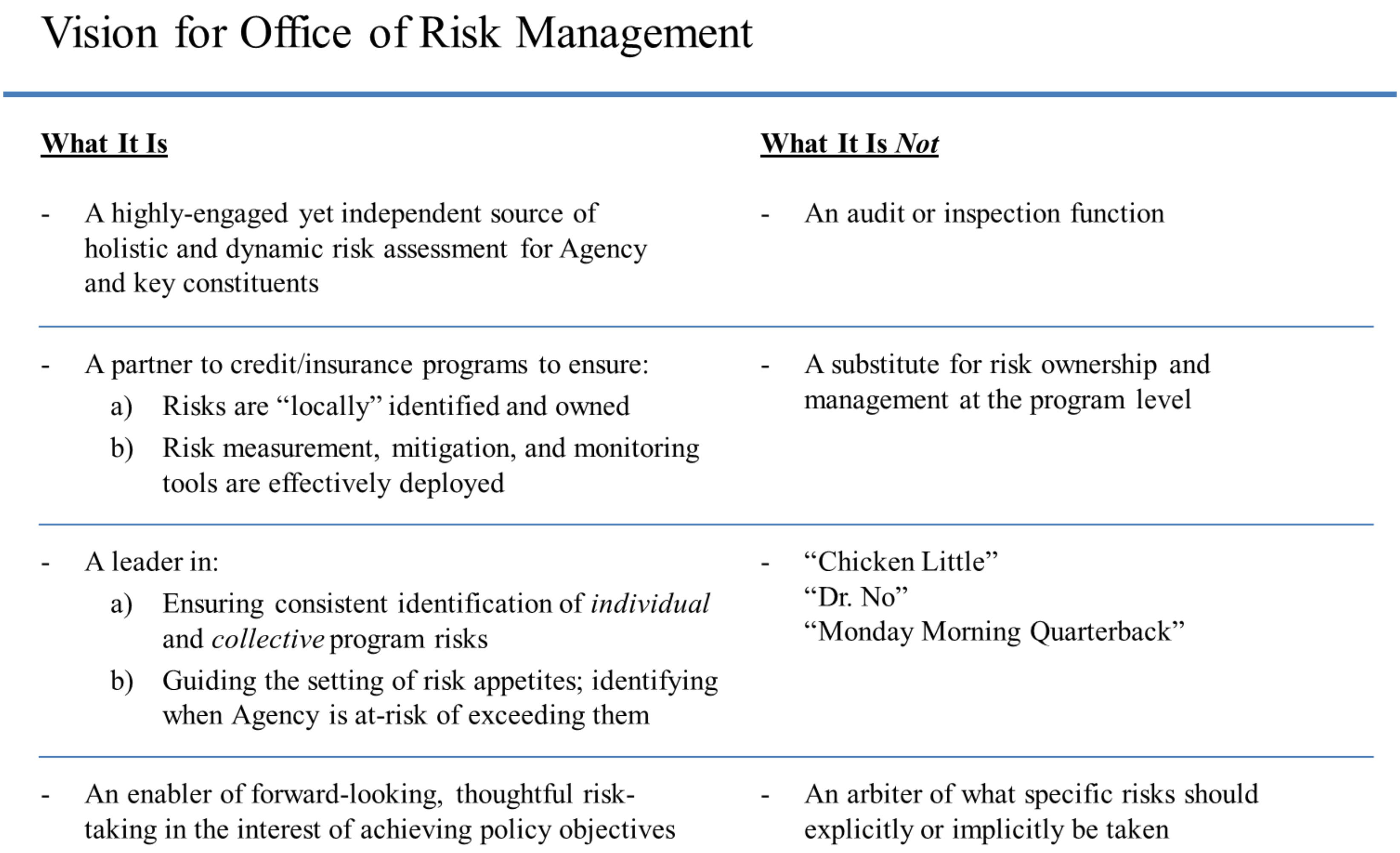
c. *Risk Committee Informal Charter (Example)*

This group will identify, track, and mitigate operational, portfolio, project, and technology risks across the organization. Representatives from the following areas will comprise the membership of this committee.

- Chief Risk Officer (chairperson)
- Chief Operating Officer (COO)
- Deputy COO
- Enterprise Performance Management Services
- Chief Financial Officer
- Chief Business Operations Officer
- Chief Compliance Officer
- Chief Customer Experience Officer
- Chief Information Officer

4. Facilitating an ERM Culture Conversation

a. Vision Statement (Example)

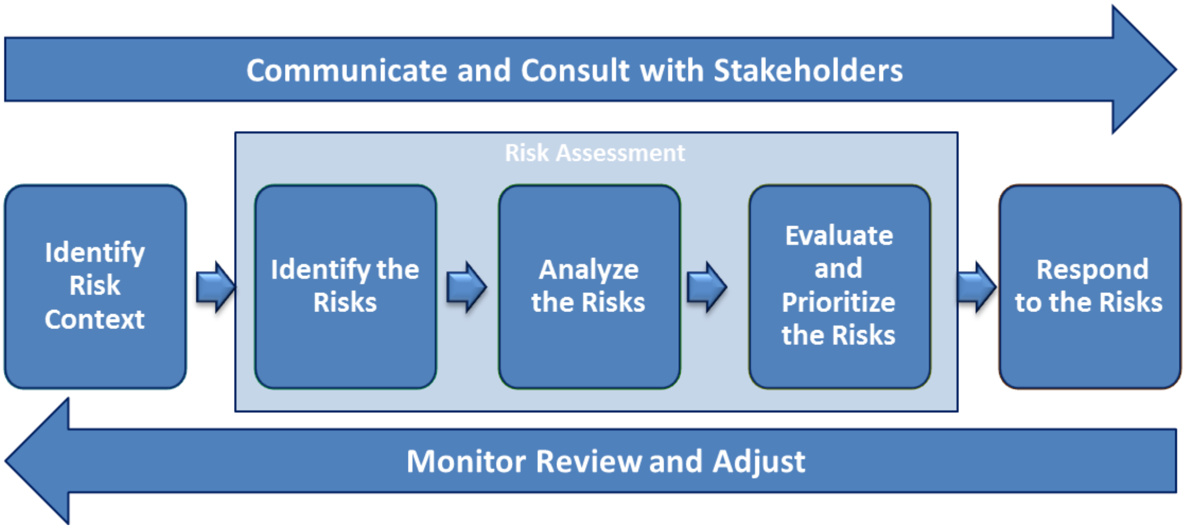


Vision for Office of Risk Management

What It Is	**What It Is *Not***
- A highly-engaged yet independent source of holistic and dynamic risk assessment for Agency and key constituents	- An audit or inspection function
- A partner to credit/insurance programs to ensure: a) Risks are "locally" identified and owned b) Risk measurement, mitigation, and monitoring tools are effectively deployed	- A substitute for risk ownership and management at the program level
- A leader in: a) Ensuring consistent identification of *individual* and *collective* program risks b) Guiding the setting of risk appetites; identifying when Agency is at-risk of exceeding them	- "Chicken Little" "Dr. No" "Monday Morning Quarterback"
- An enabler of forward-looking, thoughtful risk-taking in the interest of achieving policy objectives	- An arbiter of what specific risks should explicitly or implicitly be taken

b. ERM Policy Memo (Example)

The purpose of this memorandum is to establish an agency risk management policy. The international definition of risk is '"*the effect of uncertainty on objectives*" In [AGENCY] we define risk as *"a future event that may or may not occur and has a direct impact on the program, stewardship or organizational objectives, to their benefit or detriment."* The [AGENCY] is committed to the responsible management of risks associated with achieving our program and national objectives. The goal of risk management within [AGENCY] is to provide reasonable assurance that we understand the risks associated with achieving those objectives and that we are responding appropriately. [AGENCY] is committed to establishing an appropriate risk management culture that will contribute to good corporate governance through aconsistent risk management approach. The main elements of the [AGENCY] risk management process are depicted below.


Communicate and Consult with Stakeholders
Risk Assessment
Identify Risk Context
Identify the Risks
Analyze the Risks
Evaluate and Prioritize the Risks
Respond to the Risks
Monitor Review and Adjust

The practices of risk management within [AGENCY] are governed by the approach outlined in the risk management framework. [AGENCY] employs the risk management framework to evaluate program areas and strategic initiatives to balance risk with consideration of staffing and budget resources, stewardship and oversight responsibilities, funding within the programs, and transportation needs. The [AGENCY] risk management framework establishes a consistent process where we identify and prioritize risk and strategies to address risks. Applying the principles of risk makes it possible to identify threats and opportunities; assess and prioritize those threats and opportunities; and plan strategies to address future issues affecting agency and national objectives. In [AGENCY], risk management is a way to:

- Focus limited resources - focus staff and budget resources, to maximize opportunities and minimize events that threaten [AGENCY] programs and national objectives.
- Strengthen the ability to efficiently manage program delivery -make informed decisions about the scope, approach, and intensity of our efforts.
- Improve communication and manage risk corporately - communicate consistently about what the agency should focus on and why.

Risk management is an ongoing process, embedded in our business practices at all levels (corporate/strategic, program, unit, & project), stewardship and oversight, program management, and performance planning.

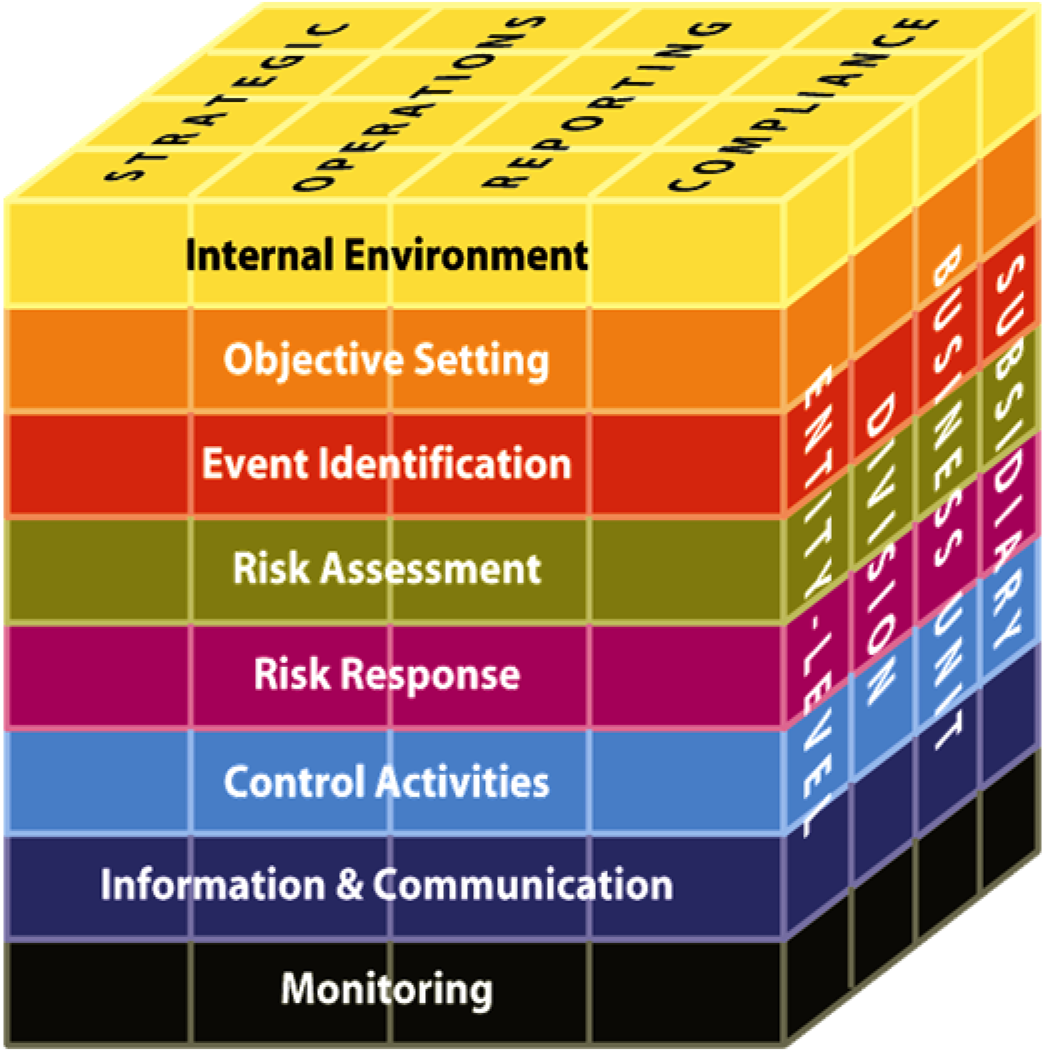
The [AGENCY] policy is to provide training, tools, and resources to assist those accountable and responsible for managing risk. All units are required to assess and report their top risks, along with associated risk response strategies annually. Agency leadership regularly monitors the status of the risk response implementation. [AGENCY] periodically reviews and improves the risk management framework.

This policy applies to all organizational units of the [AGENCY].

If you have any questions or concerns regarding the information contained in this memorandum, please contact NAME AND CONTACT INFO.

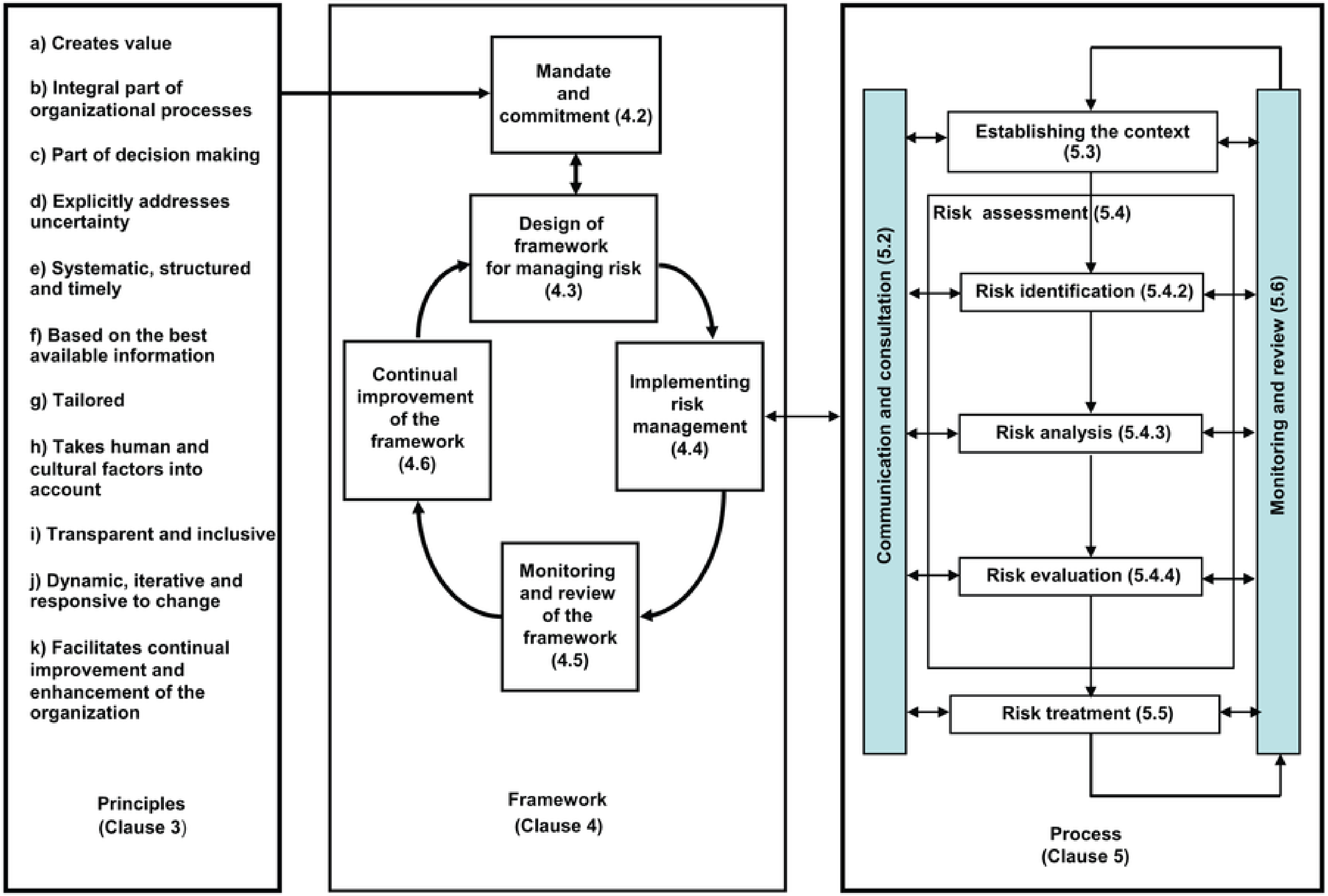
5. ERM Frameworks

a. COSO ERM Framework (Example)[8]



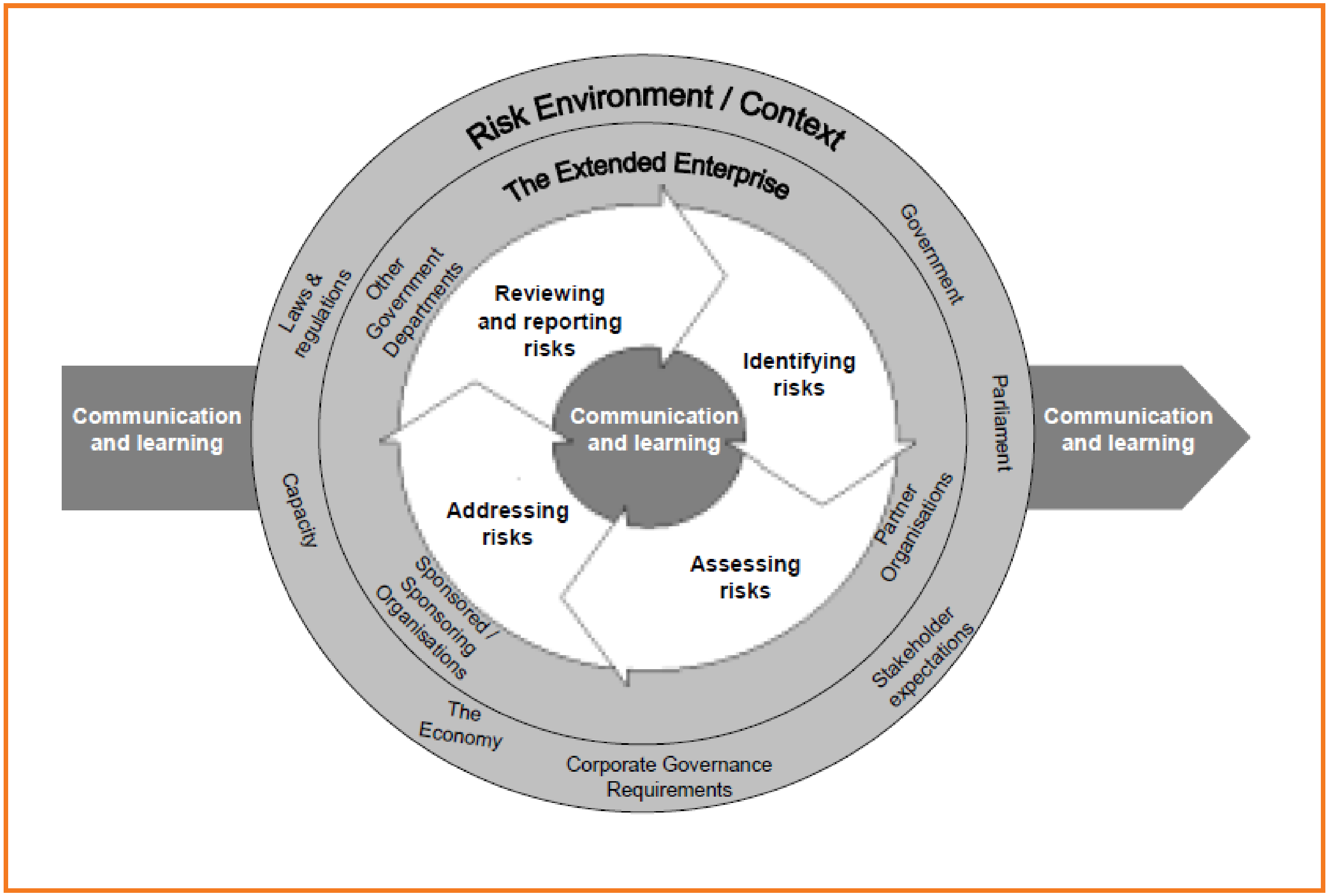
[8] Committee of Sponsoring Organizations of the Treadway Commission. Enterprise Risk Management- Integrated Framework, Executive Summary. 2004. http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf

b. ISO 31000 ERM Framework (Example)[9]


a) Creates value
b) Integral part of organizational processes
c) Part of decision making
d) Explicitly addresses uncertainty
e) Systematic, structured and timely
f) Based on the best available information
g) Tailored
h) Takes human and cultural factors into account
i) Transparent and inclusive
j) Dynamic, iterative and responsive to change
k) Facilitates continual improvement and enhancement of the organization
Principles (Clause 3)
Mandate and commitment (4.2)
Design of framework for managing risk (4.3)
Implementing risk management (4.4)
Monitoring and review of the framework (4.5)
Continual improvement of the framework (4.6)
Framework (Clause 4)
Communication and consultation (5.2)
Establishing the context (5.3)
Risk assessment (5.4)
Risk identification (5.4.2)
Risk analysis (5.4.3)
Risk evaluation (5.4.4)
Risk treatment (5.5)
Monitoring and review (5.6)
Process (Clause 5)

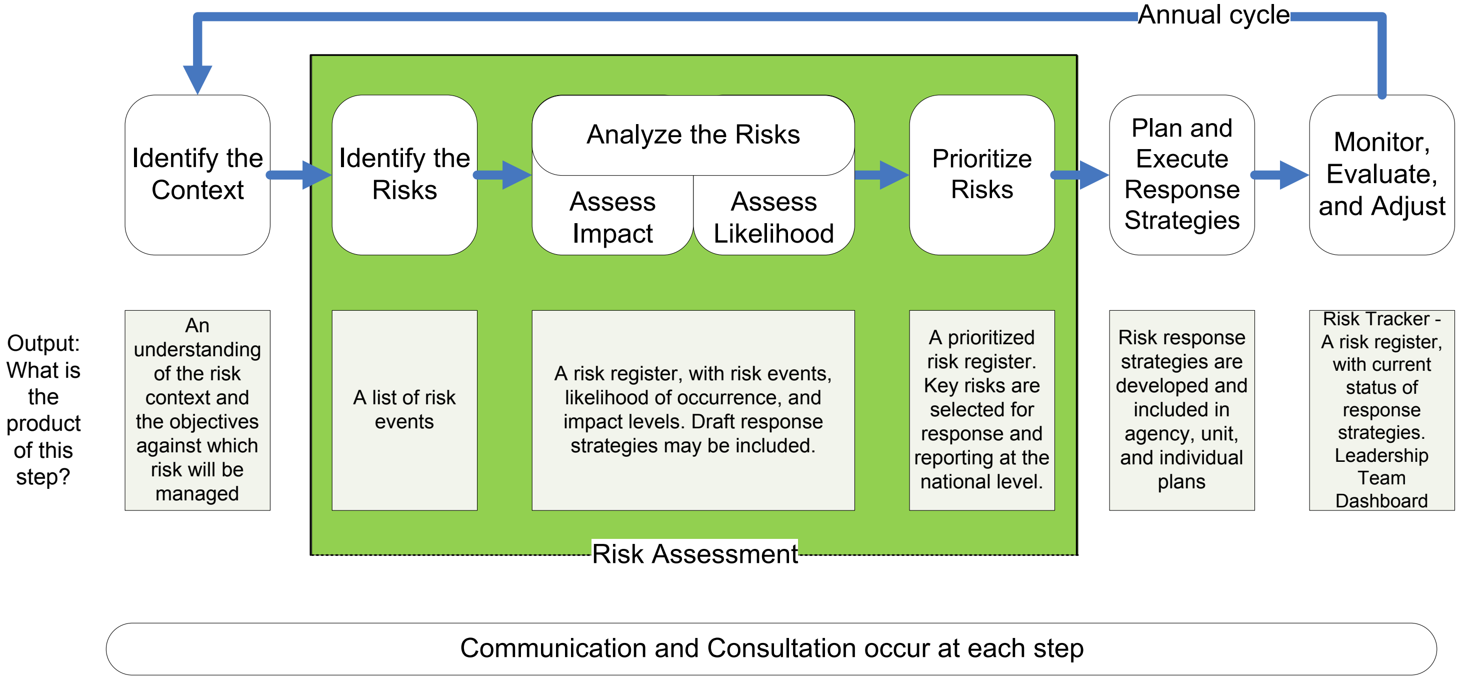
[9] International Organization for Standardization. ISO 31000:2009 Risk Management- Principles and Guidelines. 2009. https://www.iso.org/obp/ui/#iso:std:43170:en

c. *UK Orange Book ERM Framework (Example)*[10]


Risk Environment / Context
The Extended Enterprise
Communication and learning
Reviewing and reporting risks
Identifying risks
Communication and learning
Assessing risks
Addressing risks
Communication and learning
Laws & regulations
Other Government Departments
Government
Parliament
Partner Organisations
Stakeholder expectations
Corporate Governance Requirements
The Economy
Sponsored / Sponsoring Organisations
Capacity

[10] UK Treasury. The Orange Book, Management of Risk – Principles and Concepts. 2004. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf

d. *Alternative Framework (Example)*



Output: What is the product of this step?

An understanding of the risk context and the objectives against which risk will be managed

A list of risk events

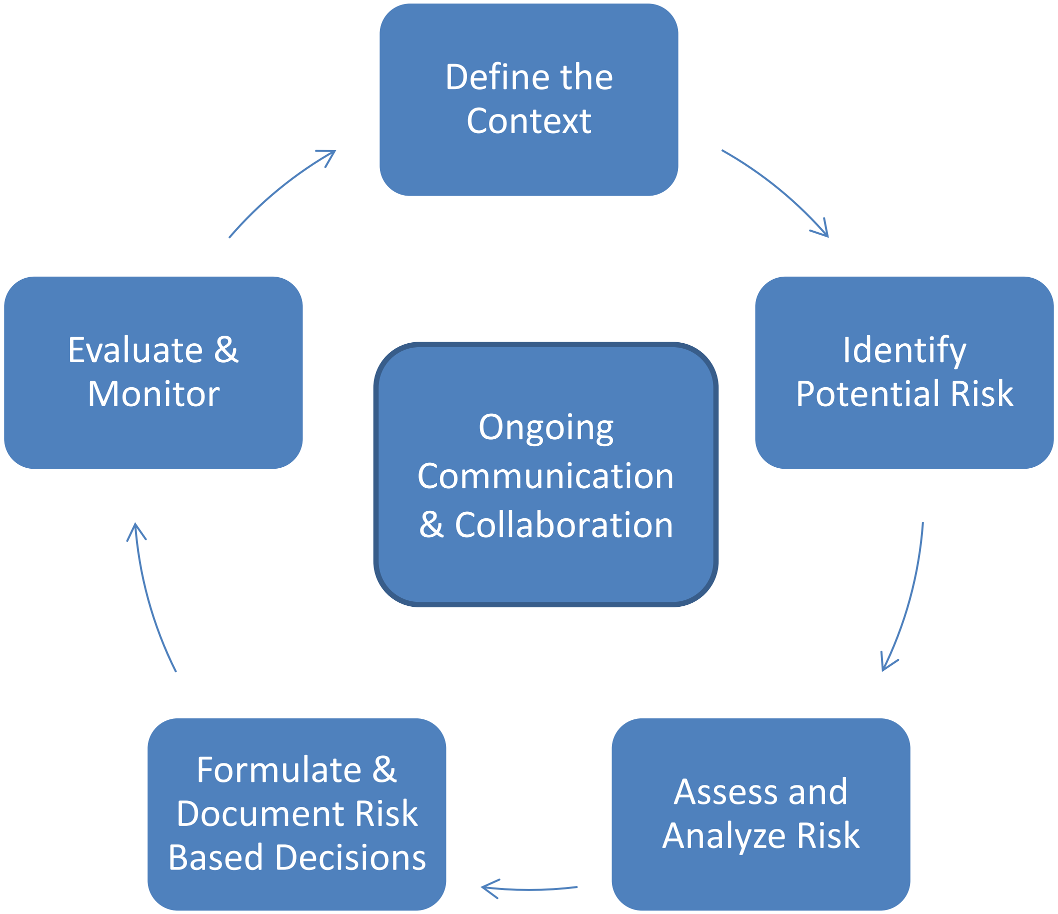
A risk register, with risk events, likelihood of occurrence, and impact levels. Draft response strategies may be included.

A prioritized risk register. Key risks are selected for response and reporting at the national level.

Risk response strategies are developed and included in agency, unit, and individual plans

Risk Tracker - A risk register, with current status of response strategies. Leadership Team Dashboard

e. Alternative Framework (Example)



6. Implementation Plans

a. *Implementation Plan (Example)*

AGENCY A-123 Implementation Plan

Governance Structure (what is currently happening or what is planned)

1. Agency has a Chief Risk Officer who reports to the (reporting chain).
2. An Office of Risk Management (ORM) supports the Chief Risk Officer (CRO). This office includes (number) Senior Policy Advisors (Grade), (number) Analysts (Grade).
3. The Agency Risk Management Committee is comprised of (describe who is on the committee). This group meets (describe frequency). (Briefly describe the meetings, what happens).
4. [Describe any other group that has been put together that feeds into the ERM process including any working groups, any groups that discuss risks across silos]

Processes for Considering Risk Appetite and Risk Tolerance Levels

1. [Describe a planned or implemented process of working with program managers to develop risk appetite and risk tolerance levels that will be approved by senior leadership on the Agency Risk Management Committee or other forum].

Methodology for Developing a Risk Profile

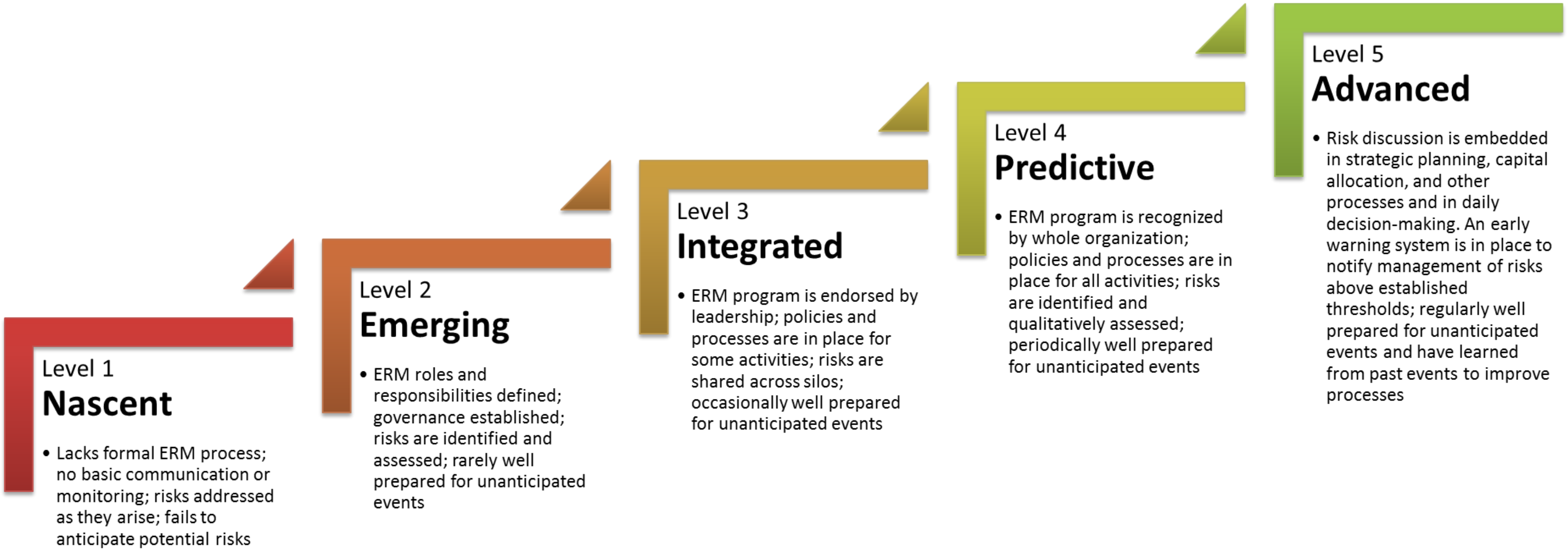
1. The Office of Risk Management will lead the identified offices and leadership team through a series of discussions to identify risks to mission, assess the likelihood and impact of those risks, prioritize accordingly and develop strategies to accept, transfer, share, avoid, or mitigate the risk and leverage opportunities.
2. Meeting 1: Risk Identification
    - Participants: CRO; Assistant Secretary/Bureau head; members of office/bureau leadership team (identified by AS/Bureau head); and ORM staff
    - Purpose: ORM will facilitate discussion of program goals and objectives and risks (internal and external) to achieving those objectives.
3. Meeting 2: Risk Assessment/Prioritization
    - Participants: ORM staff; office/bureau leadership team (as identified above)
    - Purpose: For each identified risk, ORM will facilitate discussion of the severity of the risk and potential strategies to mitigate or neutralize the risk.
4. Interim work: bureau/office leadership develop/flesh-out/validate risks and risk management strategies; ORM staff provide support as needed.
5. Meeting 3: Review and Validate Profile
    - Participants: Treasury CRO; Under Secretary; Assistant Secretaries/Bureau heads; and ORM staff
    - Purpose: Review and approve risk profiles for each office/bureau.
6. As a starting point for these meetings, ORM has consolidated risks identified by offices/ bureaus through Quarterly Performance Reviews, Strategic Objective Annual Reviews, discussions at Risk Management Committee meetings, [other].

General Timeline for Maturing the ERM Process

1. If a governance structure has not been put into place, describe when each piece is expected to be completed. If they are completed, you can discuss how long each piece has been in place.
2. If risk appetite and risk tolerance levels have not been established, describe when they are expected to be completed. If they are completed, describe how often they are reviewed and process for reviewing.
3. If a risk profile has not been completed, describe when it is expected to be completed. If it is in progress, describe progress made so far. If it has been completed, describe how often it is refreshed and process for refreshing.

7. Maturity Models

a. Five Step Maturity Model (Example)



Level 1
Nascent

- Lacks formal ERM process; no basic communication or monitoring; risks addressed as they arise; fails to anticipate potential risks

Level 2
Emerging

- ERM roles and responsibilities defined; governance established; risks are identified and assessed; rarely well prepared for unanticipated events

Level 3
Integrated

- ERM program is endorsed by leadership; policies and processes are in place for some activities; risks are shared across silos; occasionally well prepared for unanticipated events

Level 4
Predictive

- ERM program is recognized by whole organization; policies and processes are in place for all activities; risks are identified and qualitatively assessed; periodically well prepared for unanticipated events

Level 5
Advanced

- Risk discussion is embedded in strategic planning, capital allocation, and other processes and in daily decision-making. An early warning system is in place to notify management of risks above established thresholds; regularly well prepared for unanticipated events and have learned from past events to improve processes

b. Maturity Across Eleven Areas (Example)

Maturity Sub-Factors	Maturity Levels				
	1 Nascent	2 Emerging	3 Integrated	4 Predictive	5 Advanced
CULTURE					
Alignment	Failure to have congruence between the overall goals of the organization and specific units and their personnel	Select unit functions are aligned to overall goals	Relationships between all unit functions and overall goals are consistently communicated and understood by personnel	Functions across units are synchronized to support achievement of overall goals	Unit functions across the enterprise are aligned to support achievement of overall goals
Governance	Dysfunctional policies, processes, and controls with lack of even basic communication and monitoring	Governance program is established	Quality policies, processes, and controls are in place for select processes	Quality policies, processes, and controls are in place for all processes	Policies, processes, and controls are in place to protect the enterprise and are consistently communicated and monitored
PROCESS - ANALYTICAL					
Policy	No Risk Management (RM) policy is written	RM policy is written for select applications	RM policy is written for all applications	RM policy integrated into organizational policy	RM concepts are embedded in [AGENCY] policy throughout the enterprise
Method	No guidance of preferred RM methodologies	Guidance developed for select RM methodologies	Guidance developed for overall RM framework, enabling integration between processes	Interrelationships between RM processes are defined and leveraged	RM methodologies enable efficient and effective management and communication of risk across all processes and throughout the enterprise
Risk Tolerance	No formal documentation or consistent understanding of risk tolerance	Established risk tolerance for select applications	Established risk tolerance for all risk applications	Risk tolerance applied consistently for select applications	Clear identification and acceptance of risk tolerance throughout the enterprise
PROCESS - ORGANIZATIONAL					
Roles & Responsibilities	Limited formalization of RM roles and responsibilities	RM charter is written, formally establishing RM roles and responsibilities	Policy for managing risk endorsed by leadership	Organization Is fulfilling RM policy	Clear designation of RM roles and responsibilities from top to bottom and across the enterprise
Resources	Pockets of self-taught RM competence performed by part-time personnel	Some full-time RM resources supported by formal training	RM organization that is a mix of part- and full-time resources is supported by formal [AGENCY] training program	Risk duties are integrated into workforce, including position descriptions	Minimal overhead required to administer RM activities as they are performed as part of business culture

Maturity Sub-Factors	Maturity Levels				
	1 Nascent	2 Emerging	3 Integrated	4 Predictive	5 Advanced
IMPLEMENTATION					
Risk Identification, Assessment, and Communication	Risks are identified and assessed on an ad hoc basis. Uncertainty is ignored	Risk is systematically identified and assessed for select processes. Uncertainty is largely ignored	Risk data are seamlessly shared across processes. Uncertainty is expressed qualitatively for select processes	Risks are effectively and efficiently identified and qualitatively assessed across all levels of the enterprise. Uncertainty is expressed qualitatively.	Risks are effectively and efficiently identified and quantitatively assessed, including return-on-investment estimates, across all levels of the enterprise. Uncertainty is expressed quantitatively
Tools	Different tools are used by different groups to assess and manage risks for different processes	Standard tools are used across the enterprise	All RM processes use the same tools and data are integrated across select processes	All RM processes use the same tools, and data are integrated across all processes, and select processes leverage [AGENCY] enterprise data sources	RM tool is integrated with all appropriate enterprise tools and data sources
OUTCOME					
Anticipated Risks	Long history of failing to adequately address anticipated risks before they occur or expending substantial resources on relatively minor risks	Consistently failing to adequately estimate the frequency or consequence of anticipated events or over expending resources on relatively minor risks.	Consistently estimating the frequency or consequence of anticipated events and occasionally adequately managing anticipated risks and reduction of resources applied to relatively minor risks	Consistent prevention and/or adequate management of anticipated risks. Focus of resources on anticipated high-risk events	Sustained record of preventing and/or managing anticipated risks and learned from the events to avoid recurrence of related events while also integrating the information throughout the performance management process
Unanticipated Risks	Long history of failing to anticipate potential risks	Rarely executed well-prepared responses to unanticipated events	Occasionally executed well-prepared responses to unanticipated events	Periodically executed well-prepared responses to unanticipated events and learned from the events to avoid recurrence	Regularly executed well-prepared responses to unanticipated events and learned from the events to avoid recurrence of related events while also integrating the level of understanding throughout the performance management process

c. *Five Step Maturity Model (Example)*

1. **Level 1:** ***Ad hoc.*** Undocumented; in a state of dynamic change. Depends on individual heroics rather than well-defined processes.
2. **Level 2:** ***Preliminary.*** Risk is defined in different ways and managed in silos. Process discipline is unlikely to be rigorous.
3. **Level 3:** ***Defined.*** A common risk assessment/response framework is in place. An organization-wide view of risk is provided to executive leadership. Action plans are implemented in response to high priority risks.
4. **Level 4:** ***Integrated.*** Risk management activities are coordinated across business areas. Common risk management tools and processes are used where appropriate, with enterprise-wide risk monitoring, measurement, and reporting. Alternative responses are analyzed with scenario planning. Process metrics are in place.
5. **Level 5:** ***Optimized.*** Risk discussion is embedded in strategic planning, capital allocation, and other processes and in daily decision-making. An early warning system is in place to notify the board and management of risks above established thresholds.

C. Risk Assessment

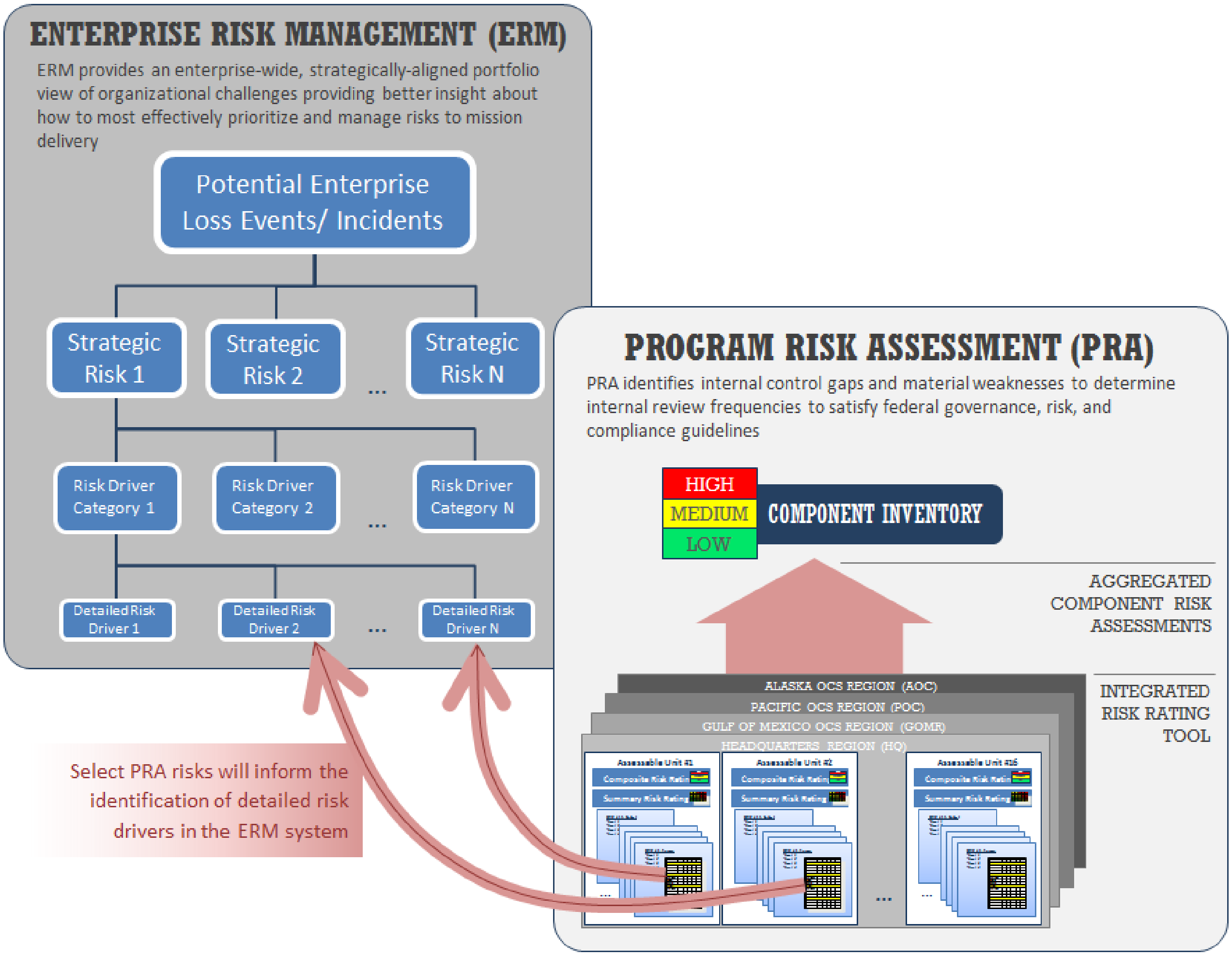
1. Establishing Context

a. Defining Context (Example)

Key Steps in Defining Context When Applying Risk Management Principles	
Risk Tolerance and Risk Appetite	Risk management efforts often involve tradeoffs between positive and less positive/ideal outcomes. Having a current and accurate perspective on an organization and decision makers' risk tolerance and risk appetite will help shape the assessments and the development of actionable risk management alternatives.
Scope & Criticality of the Decision	Understand the decision or range of decisions that have to be made and the range of options available to leaders. Also consider the breadth and depth of the decision's impact. The risk analysis and effort should be commensurate to that criticality.
Establish Goals & Objectives	Ensure that the goals and objectives of the project and risk management analysis align with the desired requirements, outcome, or end-state of the decision making process. Clearly defined goals and objectives are essential for identifying, assessing and managing risks.
Decision Timeframe	Consider the timeframe in which a decision must be made, socialized and executed including time available for conducting formal analysis and decision review.
Resources and Risk Management Capabilities	Identify the staffing, budget, skill sets/expertise, and other resources available for successful project completion including risk analysis and risk management efforts. Resources applied should be commensurate with the complexity of the issues involved and the magnitude of the decision.
Availability and Quality of Information	Consider the availability and quality of information that exists within the Agency or that can be accessed as needed, based on the design of the risk analysis approach, the time available for analysis and other factors. In engaging with decision makers at the outset of a risk based analysis cycle, it is important to convey anticipated data limitations, including expected levels of data availability.
Decision Makers and Stakeholders	Organizational leaders must be engaged at the beginning of a risk management/analysis process so the approach and presentation of results are tailored to their preferences and the analysis is responsive to the breadth of issues upon which they're seeking guidance.
Policies and Standards	Ensure risk management efforts utilize, complement and take into account any risk management policies, standards or requirements the Agency already has in place. The Enterprise Risk Management program is designed to leverage and complement these and other existing processes to identify monitor and mitigate risk.

2. Risk assessments and the ERM Process

a. Using Risk Assessments to Inform the ERM Process (Example)



ERM provides an enterprise-wide, strategically-aligned portfolio view of organizational challenges providing better insight about how to most effectively prioritize and manage risks to mission delivery

PRA identifies internal control gaps and material weaknesses to determine internal review frequencies to satisfy federal governance, risk, and compliance guidelines

Select PRA risks will inform the identification of detailed risk drivers in the ERM system

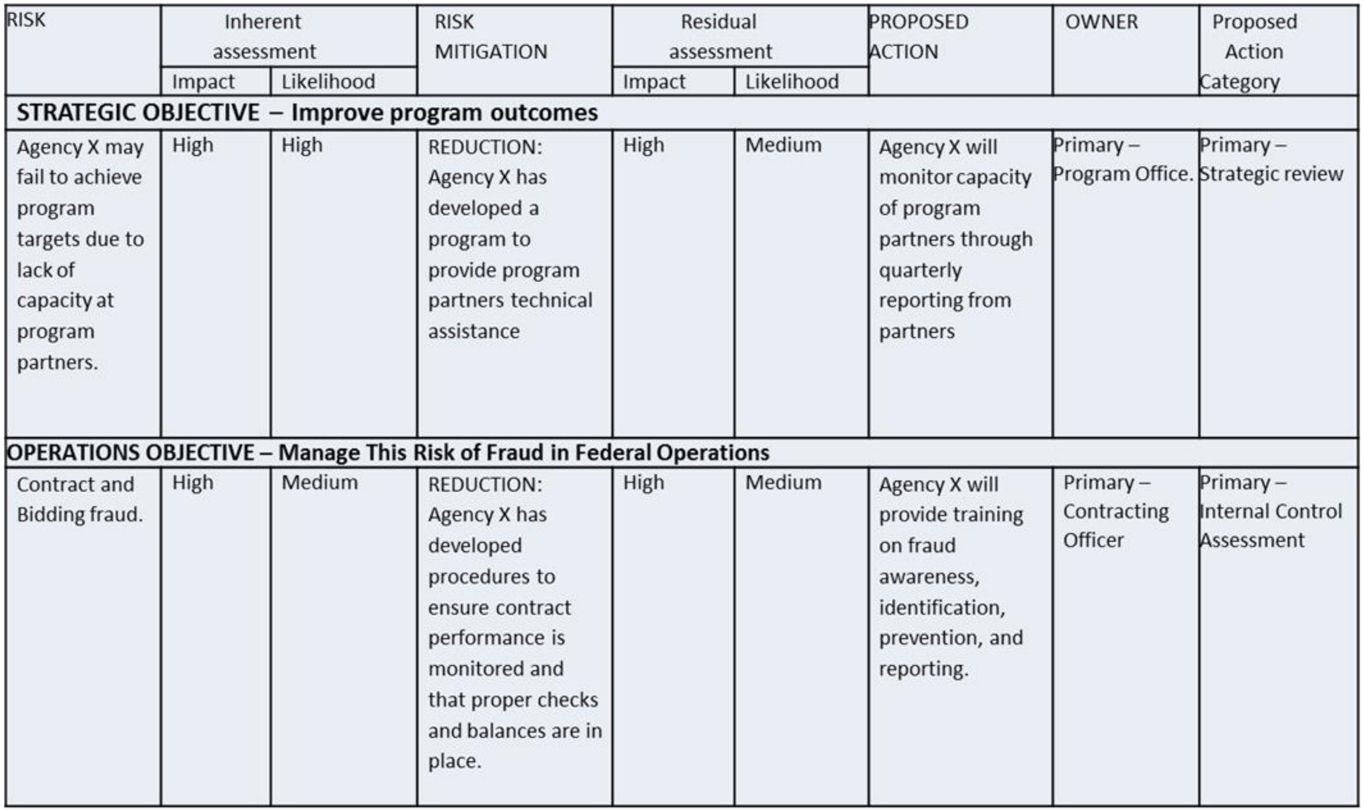
D. Risk Profile

1. Key Questions to Help Develop a Risk Profile

Step	Questions
1. Communication and Consultation	• Who needs to be involved? • How will we communicate and consult with them?
2. Identify Risk Context	• What are your objectives? • What are the things to consider when we assess the risks of achieving our objectives? • What criteria will we use to assess our risks? • Who will do the assessment?
3. Identify the Risks	• What events could happen that would affect my program areas or objectives? • What are the corresponding impacts?
4. Analyze the Risks	• What is the severity of this impact according to accepted agency criteria? • What is the likelihood that this risk event will occur?
5. Prioritize the Risks	• What are the impact level and likelihood of your risks? • How do the risks compare, such as on heat-map? • Which risks does leadership consider the “top risks?” • Which risks will require a response?
6. Identify and Prioritize Risk Responses	• What actions will we take to mitigate, avoid, accept, transfer, or enhance our risks? • What actions are important to take now? • Are there ongoing actions to continue? • Who is accountable, when will they start, and when will it be done?
7. Monitor, Evaluate, and Adjust	• What is the status of our response actions? • Are they completed, in progress, not started, or has the action been deferred? • Did the action have the desired effect? What is the residual risk and how should we respond?

2. Templates

a. Sample Risk Profile #1



RISK	Inherent assessment		RISK MITIGATION	Residual assessment		PROPOSED ACTION	OWNER	Proposed Action Category
	Impact	Likelihood		Impact	Likelihood			
STRATEGIC OBJECTIVE – Improve program outcomes								
Agency X may fail to achieve program targets due to lack of capacity at program partners.	High	High	REDUCTION: Agency X has developed a program to provide program partners technical assistance	High	Medium	Agency X will monitor capacity of program partners through quarterly reporting from partners	Primary – Program Office.	Primary – Strategic review
OPERATIONS OBJECTIVE – Manage This Risk of Fraud in Federal Operations								
Contract and Bidding fraud.	High	Medium	REDUCTION: Agency X has developed procedures to ensure contract performance is monitored and that proper checks and balances are in place.	High	Medium	Agency X will provide training on fraud awareness, identification, prevention, and reporting.	Primary – Contracting Officer	Primary – Internal Control Assessment

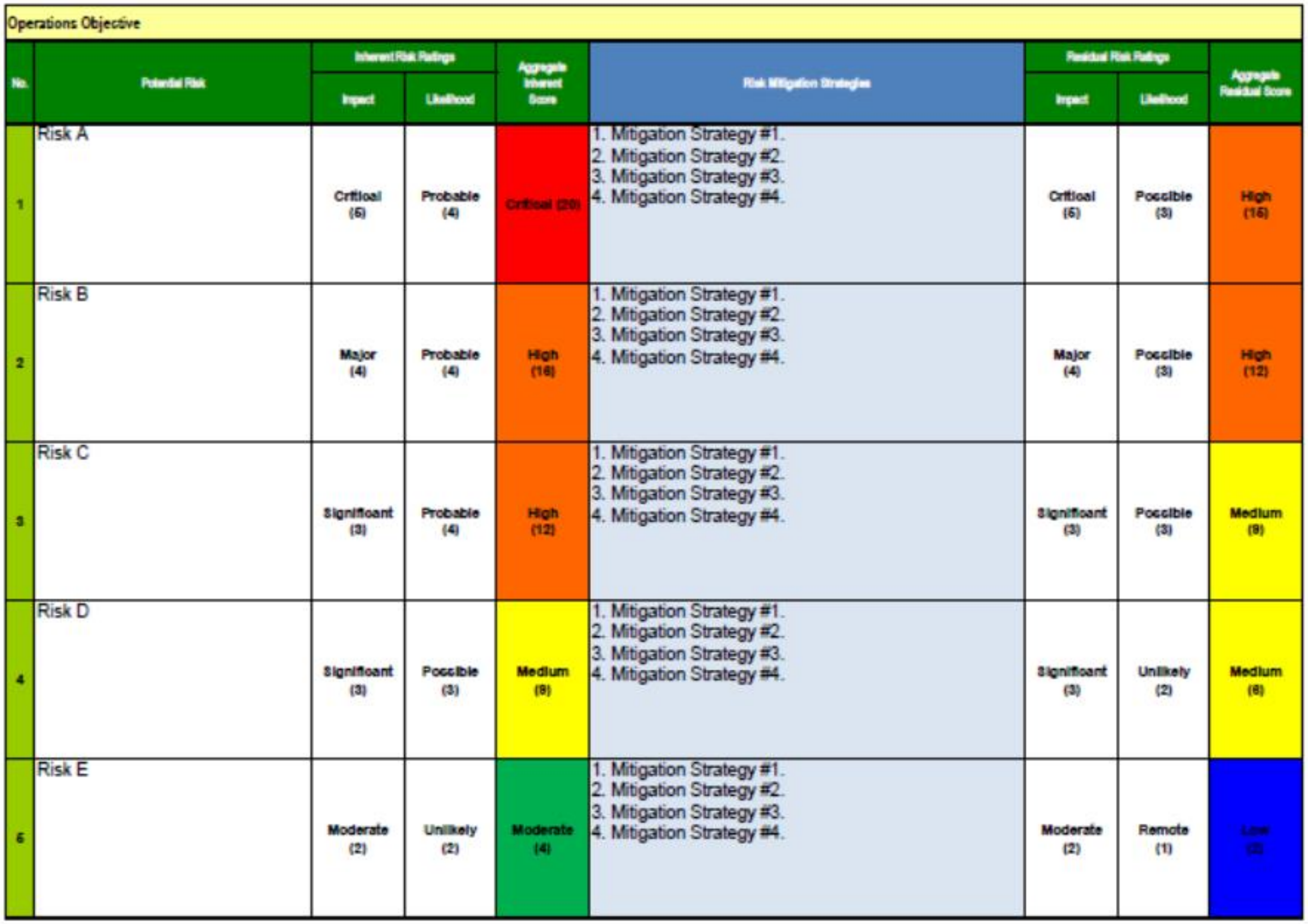
b. Sample Risk Profile #2

Risk Short Description	Risk Event	Primary Impact	Threat or Opportunity	Likelihood	Impact Category	Order of Priority	Response Strategy Type	Response Strategy

c. Sample Risk Profile #3

Program Office/ Contact	Risk Short Name	Mission Area/ Objective	Risk Short Description	Mitigation Strategy	Current Status	Key Stakeholders	Risk Type/ Category	Likelihood (1-5)	Impact (1-5)	Source	Notes

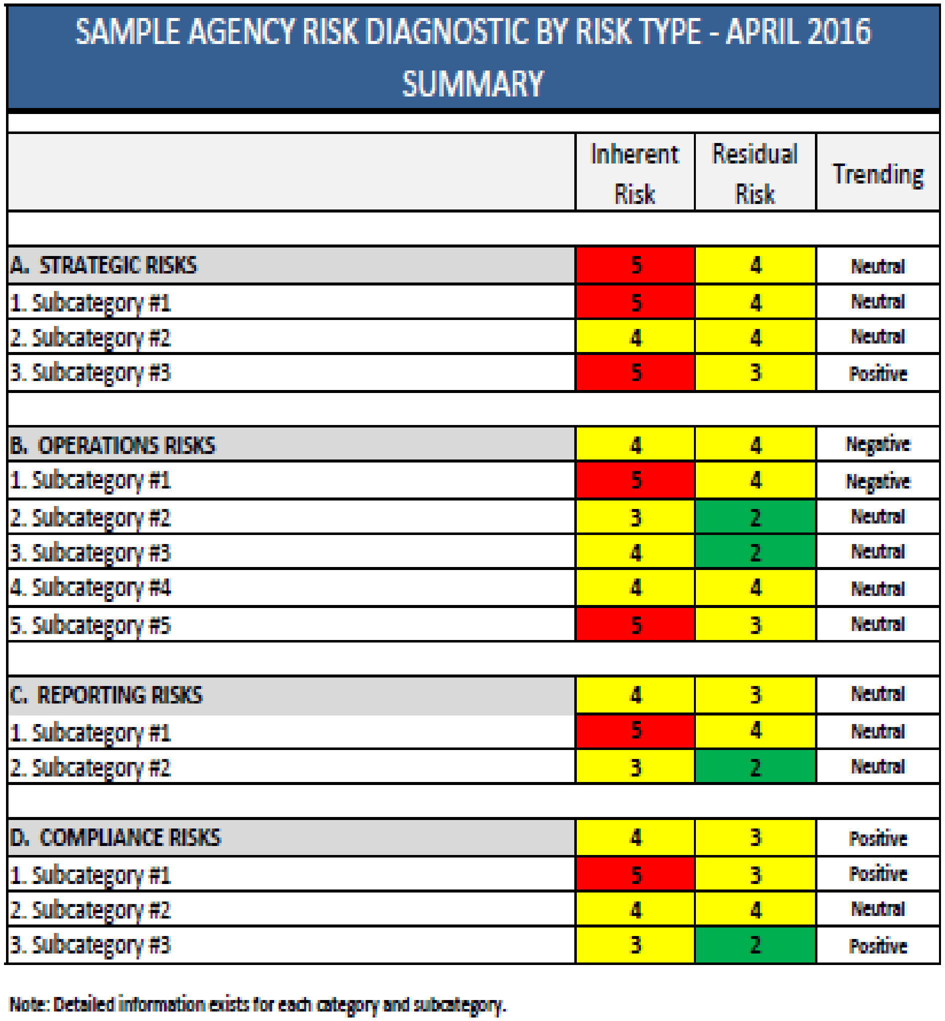
d. *Sample Risk Profile #4*



Operations Objective

No.	Potential Risk	Inherent Risk Ratings		Aggregate Inherent Score	Risk Mitigation Strategies	Residual Risk Ratings		Aggregate Residual Score
		Impact	Likelihood			Impact	Likelihood	
1	Risk A	Critical (5)	Probable (4)	Critical (20)	1. Mitigation Strategy #1. 2. Mitigation Strategy #2. 3. Mitigation Strategy #3. 4. Mitigation Strategy #4.	Critical (5)	Possible (3)	High (15)
2	Risk B	Major (4)	Probable (4)	High (16)	1. Mitigation Strategy #1. 2. Mitigation Strategy #2. 3. Mitigation Strategy #3. 4. Mitigation Strategy #4.	Major (4)	Possible (3)	High (12)
3	Risk C	Significant (3)	Probable (4)	High (12)	1. Mitigation Strategy #1. 2. Mitigation Strategy #2. 3. Mitigation Strategy #3. 4. Mitigation Strategy #4.	Significant (3)	Possible (3)	Medium (9)
4	Risk D	Significant (3)	Possible (3)	Medium (9)	1. Mitigation Strategy #1. 2. Mitigation Strategy #2. 3. Mitigation Strategy #3. 4. Mitigation Strategy #4.	Significant (3)	Unlikely (2)	Medium (6)
5	Risk E	Moderate (2)	Unlikely (2)	Moderate (4)	1. Mitigation Strategy #1. 2. Mitigation Strategy #2. 3. Mitigation Strategy #3. 4. Mitigation Strategy #4.	Moderate (2)	Remote (1)	Low (2)

e. *Sample Risk Profile #5*



SAMPLE AGENCY RISK DIAGNOSTIC BY RISK TYPE - APRIL 2016 SUMMARY	Inherent Risk	Residual Risk	Trending
A. STRATEGIC RISKS	5	4	Neutral
1. Subcategory #1	5	4	Neutral
2. Subcategory #2	4	4	Neutral
3. Subcategory #3	5	3	Positive
B. OPERATIONS RISKS	4	4	Negative
1. Subcategory #1	5	4	Negative
2. Subcategory #2	3	2	Neutral
3. Subcategory #3	4	2	Neutral
4. Subcategory #4	4	4	Neutral
5. Subcategory #5	5	3	Neutral
C. REPORTING RISKS	4	3	Neutral
1. Subcategory #1	5	4	Neutral
2. Subcategory #2	3	2	Neutral
D. COMPLIANCE RISKS	4	3	Positive
1. Subcategory #1	5	3	Positive
2. Subcategory #2	4	4	Neutral
3. Subcategory #3	3	2	Positive

Note: Detailed information exists for each category and subcategory.

f. Sample Risk Profile #6

Significant Operational Issues Dashboard

		DATE		**DATE**		
		Risk Impact	**Likelihood of Occurrence**	**Risk Impact**	**Likelihood of Occurrence**	**Trending**
Current Risks	**Mitigation Strategies**	-	-	-	-	-
A. Sample Risk #1	● Mitigation Strategy #1. ● Mitigation Strategy #2. ● Mitigation Strategy #3.	3	2	3	2	**Neutral**
B. Sample Risk #2	● Mitigation Strategy #1. ● Mitigation Strategy #2. ● Mitigation Strategy #3.	3	3	3	4	**Negative**
C. Sample Risk #3	● Mitigation Strategy #1. ● Mitigation Strategy #2. ● Mitigation Strategy #3.	5	4	5	3	**Positive**
D. Sample Risk #4	● Mitigation Strategy #1. ● Mitigation Strategy #2. ● Mitigation Strategy #3.	2	3	2	3	**Neutral**
E. Sample Risk #5	● Mitigation Strategy #1. ● Mitigation Strategy #2. ● Mitigation Strategy #3.	5	2	5	3	**Negative**
F. Sample Risk #6	● Mitigation Strategy #1. ● Mitigation Strategy #2. ● Mitigation Strategy #3.	4	5	4	3	**Positive**

3. Risk Assessment Tools

a. Example #1

Likelihood Scale

Likelihood	Definition
1 - Very Low	Risk event **rarely** to occur, or occurs less than once every 10 years.
2- Low	Risk event **unlikely** to occur, or occurs less than once a year, but more than once every 10 years.
3- Medium	Risk event **possible** to occur, **or** occurs between 1-10 times a year.
4. High	Risk event **highly likely** to occur, **or** occurs between 11-50 times a year.
5- Very High	Risk event **almost certain** to occur, **or** occurs > 50 times a year

Impact Scale on Quality of Operations/Activity/Mission

Measured Impact	1 - Very Low	2 – Low	3 – Moderate	4 - High	5 - Very High
Reduced quality and performance	Degradation in Activity/Role is negligible	Degradation in Activity/Role is noticeable	Degradation in Activity/Role has Material Impact on Performance of Key Function(s)	Degradation in Activity or Role Requiring Escalation	Degradation of Activity or Role Severely Impacts Key Deliverable or Performance Measure

.

Risk Prioritization Matrix based on Calculated Risk Score (**Likelihood x Impact**)

	Likelihood of Incident Scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	1	2	3	4	5
	Low	2	4	6	8	10
	Moderate	3	6	9	12	15
	High	4	8	12	16	20
	Very High	5	10	15	20	25

Likelihood Score: *Ranges from Very Low (1) to Very High (5)*. Risk likelihood refers to the overall likelihood of the occurrence and should consider the presence and effectiveness of controls to mitigate risks.

Impact Score: *Ranges from Very Low (1) to Very High (5)*. Risk impact refers to the presumed impact if the risk becomes reality.

Overall Risk Score: Risk scores are derived by multiplying the value identified for likelihood by the value identified as the potential impact if a risk materialized.

(Example: Risk Likelihood Score of 3 with Estimated Impact Score of 4 = Medium Risk Prioritization Rating of 12)

High Priority	15 - 25	🟥
Medium Priority	5 - 14	🟨
Low Priority	1 - 4	🟩

b. Example #2

Likelihood Criteria

	Staffing (Levels & Experience)	Operational Procedures	Guidance	Problem History	New Program, Phase or Component	Complexity	Outside Control	Potential for Waste, Fraud and Abuse	Work Force Development and Training	Agency Involvement	Consultant Use	Other
Likelihood Level	Is the staff assigned to the effort sufficient? Do they have a clear knowledge, understanding, and ability with the program area or objective and its implications	Are there documented and relevant procedures for this program area or objective of the program?	Is there relevant guidance?	Have there been significant problems or ongoing series of problems related to this program area or objective?	Is program area or objective of the program is truly novel?	Is there a high level of intricacy or challenge associated with the program area or objective?	Is there an opportunity for outside agencies to assert control or interference?	What is the opportunity waste, fraud, and abuse?	Is there program in place to keep training and development in place for the personnel related to this program area or objective?	Is our division office staff actively is involved in managing the program area or objective?	Are consultants actively being applied as primary resources in the effort?	Are there other areas of concern related to this program area or objective that are not addressed in the frequency criteria? (Document the criteria below)
Almost Certain	Severely understaffed or no experience: It is unrealistic to expect the staff assigned not to need supplementation or augmentation before the end of the effort	None: There are no documented or relevant procedures	None: There are no documented or relevant guidance	A lot of: There are historical events that tie directly to the problem history	Cutting Edge: No one has addressed this type of work in this program area or objective before	Almost Certain: The program area or objective involves integration of multiple agencies, consultants and contractors	Almost Certain: Numerous outside agencies and the public have the opportunity and ability to voice concerns, influence or direct	A lot of: There is almost no oversight and a almost no ability to identify waste, fraud and abuse	None: There are no training or mentoring programs	None: Division office personnel have no visibility or no management control	A lot of: The Agency is using a broad range of consultant to address the program area or objective	
Likely	Understaffed or no experience: Staff assigned will be over utilized and likely incapable of completion of with out immediate training.	Some: There are some documented procedures or tangentially related procedures	Some: There is some documented guidance or tangentially related guidance	Some: There have been some incidents of problems related to this program area or objective in this type of program	Done in other transportation agencies: This type of work has been done in other transportation agencies, but no experience at this agency	Likely: The program area or objective involves integration of multiple agencies	Likely: One or two outside agencies and the public have the opportunity and ability to voice concerns, influence or direct	Some: There is some oversight, but certain gaps in our ability to identify waste, fraud and abuse	Limited: There are training and/or mentoring programs, but no funding and/ or leadership commitment	Limited: Division office personnel have visibility but no management control	Some: The Agency is sharing significant responsibilities with consultants related to this program area or objective	
Possible	Understaffed or some experience: Staff assigned will be over utilized and run the risk of being incapable of completion if additional responsibilities are assigned, or lack experience	Out-of-date: There are documented procedures, but they are out-of-date with existing laws and regulations.	Out-to-date: There are documented guidance, but they are out-of-date with existing laws and regulations.	Possible: There are rumors or organizational legend of problems related to this program area or objective in this type of program	Some experience: Some people have done this type of work in the past or have done related work	Possible: This program area or objective involves integration of Agency and one other outside agency	Possible: One or two outside agencies have the opportunity and ability to voice concerns, influence or direct	Possible: There is oversight, but possible gaps in our ability to identify waste, fraud and abuse	Some: There are training and/or mentoring programs, but they are not universally available	Some: Division office personnel have management control over some aspects of the program area or objective	Limited: The Agency is sharing limited responsibilities with consultants related to this program area or objective	
Unlikely	Adequately staffed or competent: Adequately staffed or competent	Good and up-to-date: Procedures are good and up to date.	Good and up-to-date: Guidance is good and up to date.	None: There have been no significant or ongoing problems.	Old news: It's what we do, routine	Unlikely: This program area or objective involves only Agency personnel	Unlikely: There is virtually no opportunity or ability for outside agencies to voice concerns related to this program area or objective	None: There is virtually total oversight and a high opportunity to identify waste, fraud and abuse	A lot of: There are training and mentoring programs, broadly available to personnel	A lot of: Division office personnel have active management control over most aspects of the program area or objective	None: The Agency has full responsibility for all aspects of this program area or objective	

Impact Criteria

	Financial	Reputation	Business Operations	Legal and Compliance	Infrastructure Assets	Resources and Effort Required	Human and Natural Environment	Safety	Civil Rights	Economic
Catastrophic	Large unacceptable financial loss, severe budget variance. Critical long term impact on budget/finances, not recoverable within current or next fiscal year. Critical business functions could be vulnerable or ineligible. Systematic and extensive major fraud. Results in qualified audit opinion.	Very significant harm to image with substantial impact on effectiveness. Significant adverse community impact and condemnation. Consistent extreme negative media attention (months). Irreconcilable community loss of confidence in the organization's intentions and capabilities and possibly in the government. Secretary level intervention	Large and unacceptable operational impact, long term business interruption. System failure and overall survival of the organization is threatened. Full business disruption for more than one week or a key service more than two weeks. Majority of critical programs cannot be achieved. Secretary level intervention	Material compliance infraction. Significant prosecution and fines. Major litigation involving class actions. Major non-compliance with legislation.	Significant or critical infrastructure assets are destroyed. Significant or critical infrastructure assets are unusable for months.	Impact cannot be managed within the organization's existing resources and threatens the survival of the organization. Department Secretary level intervention.	The event will permanently affect the human and natural environment. The impact covers a wide area and is difficult to contain. The effects are irreversible. Threat to survival of flora, fauna, and or cultural heritage.	Many fatalities.	Program or critical component of a program declared unconstitutional the US Supreme Court, thereby effectively eliminating it nationally. Complete inability to achieve any of the program's objectives, or any objectives of a critical component of a program.	Significant, long lasting negative impacts to the economy of a major metropolitan area, a State or the nation
Major	Very significant financial loss, major budget variance. Significant impact on budget/finances/eligibility, not recoverable within current or next fiscal year. Significant fraud waste or abuse. Leads to material weakness.	Major embarrassment leading to significant impact on effectiveness. Considerable and prolonged community impact and dissatisfaction publicly expressed Community loss of confidence in the organization's and capabilities (weeks) Consistent negative media attention (weeks) Administrator or Executive Director level intervention	Unacceptable operational impact, short term business interruption. Continued capability of the organization is threatened. Full business disruption for up to one week or a key service up to two weeks. One or more critical programs, projects, or agency priorities cannot be achieved	Reportable compliance infraction. Major breach of regulations. Major litigation.	Non critical infrastructure assets are destroyed. Significant or critical infrastructure assets are unusable or restricted for weeks.	Impact requires significant long term management and organizational resources to respond.	Medium to long term impact to the the human and natural environment. The impact covers a wide area but can be contained. Able to be remediated but will require dedicated expert resources.	Fatalities or permanent disabilities.	Long-term impact on the protected rights, intended benefits, or ability to implement effective nondiscrimination programs. Numerous and continuous complaints in multiple program areas that cannot be addressed timely.	Significant economic disruption to a major metropolitan area or entire State
Moderate	Significant financial loss and variance to budget. Major impact on budget/finances/eligibility, may be recoverable within current year, but requires reprioritization. Limited instances fraud waste or abuse. Leads to several audit findings.	Moderate embarrassment impacting short term effectiveness. Community impact and concerns publicly expressed (days) Negative media attention (days) Loss of confidence by the community in organization processes Administrator or Executive Director level concern	Moderate operational impact, business not interrupted. Effectiveness and efficiency of major elements of the organization are reduced. Full business disruption for one day or a key service disruption up to one week. Ability to achieve one or more critical programs, projects, or agency priorities is reduced.	Significant compliance infraction. Serious incident requires investigation and legal representation to determine legal liability. Non compliance with regulation.	Some assets, not including significant or critical assets, are unusable or restricted for weeks.	Impact requires management and resources from a key area of the organization to respond.	Medium term impact to the the human and natural environment. Limited to a small area. Able to be remediated but will require intervention or management by external parties.	Injuries requiring medical treatment with possible fatalities.	Impact results in noncompliance affecting protected rights or intended benefits. Issues are addressed, but over unreasonably long period of time. Numerous complaints in one or more program areas.	Some economic disruption to a metropolitan area or portion of a State; impacts may or may not be long lasting
Minor	Minor financial loss, small budget variance. Slight but noticeable impact on budget/finances/eligibility, recoverable within year. Minor instances of fraud waste or abuse. Leads to audit findings.	Minor embarrassment, but no harm to image or reputation. Local community impact and concerns Occasional or once off negative media attention	Minor operational impact, business not interrupted. Effectiveness and efficiency elements of the organization are reduced, Partial business disruption for less than three days. Opportunity or ability to achieve objectives or deliver outcomes is affected.	Minor compliance infraction. Complex legal issue to be addressed.	A number of assets are unusable or restricted but can be replaced within an acceptable timeframe.	Impact requires additional local management effort and redirection of resources to respond.	Short term impact to the the human and natural environment. Able to be remediated through existing processes. Minimal threat to flora, fauna, and or cultural heritage	Injuries requiring medical treatment.	Minor impact on protected rights or intended benefits with isolated lawsuits and/or complaints that do not involve cross-cutting program issues.	Some economic disruption to a metropolitan area or portion of a State, but effects are both manageable and short term
Insignificant or Neutral	Minimal impact on budget/finances/eligibility. Recoverable within current year. Some waste or abuse. Leads to immaterial audit findings.	Isolated local community or individual issue-based concerns	Negligible impact on the effectiveness of the organization. Isolated or short term business service disruption.	Legal issues managed by routine procedures.	Assets receive minimal damage or are only temporarily unavailable or restricted.	Impact can be managed through routine activities.	No measurable impact to the the human and natural environment. No action required for management or containment. No impact to flora, fauna, and or cultural heritage.	Incident with or without minor injury.	No measureable impact to protected rights or intended benefits of individuals.	Some localized, short-term economic disruption

Heat Map

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

c. *Example #3*

Likelihood Criteria

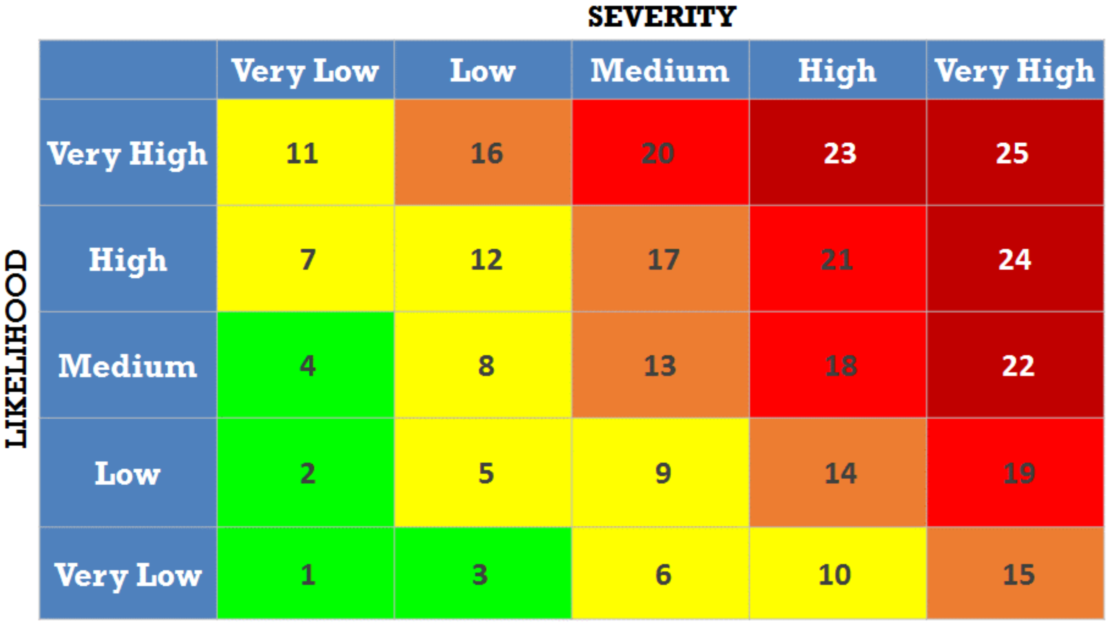
Likelihood Level	Time Basis			
	Numerically Based		Event Based	
	Numerical Boundaries	Representative Value	Operational Benchmark	Internal
Very High	Expect to see once per year or more	2/yr	Example: Lifting incidents Highest Severity • Safe: Two or fewer deaths • Clean: Spill of 20,000 bbls or less	Example: Inability to meet some activity-based targets
High	Expect to see between once per year and once in 10 years	0.2/yr	Example: Black Elk Highest Severity • Safe: 2 to 10 deaths • Clean: Spill of 20,000 to 100,000 bbls	Example: Senior staff is replaced and some internal reorganization occurs
Medium	Expect to see between once in 10 years and once in 100 years	0.02/yr	Example: *Deepwater Horizon* tragedy Highest Severity • Safe: 10 to 100 deaths • Clean: Spill of 100,000 to 500,000 bbls	Example: Fundamental inability to successfully perform key mission elements and requiring complete re-commissioning of personnel and management systems
Low	Expect to see between once in 100 years and once in 1,000 years	0.002/yr	Example: Major releases from multiple sites following hurricane Highest Severity • Safe: 100 to 1,000 deaths • Clean: 500,000 to 5 million bbls	Example: Having severe challenges to performing mission (like the Nuclear Regulatory Commission at time of Three Mile Island) and needing some new leadership with substantial reorganization and updating of management systems
Very Low	Expect to see less than once in 1,000 years	0.0002/yr	Example: Major releases from more than 20 sites following earthquake/tsunami Highest Severity >5 million	Example: Completely unable to perform mission and requiring complete re-commissioning with new leadership and complete re-organization with new management systems and/or alignment at the Federal government level

Impact Criteria

Severity Category	External Impact or Consequence Type				Internal Impact
	Safe	Clean	Economic	Reputation	
Very High		> 5 million bbls of crude oil released	> $100 Billion		Completely unable to perform mission and requiring complete re-commissioning with new leadership and complete re-organization with new management systems (Mission impacts exceeding the Deepwater Horizon impacts)
High	>1,000 deaths	500,000 to 5 million bbls of crude oil released	$10 Billion to $100 Billion	Multiple formal investigations (e.g., Congressional investigative hearing; OIG and GAO investigations); prolonged national media coverage; industry/public outrage and loss of confidence in [AGENCY] to perform its mission.	Severe challenges to performing mission and needing some new leadership with substantial reorganization and updating of management systems (Mission impacts between one-tenth to up to the Deepwater Horizon impacts)
Medium	100 to 1,000 deaths	100,000 to 500,000 bbls of crude oil released	$1 Billion to $10 Billion	Congressional investigative hearing; OIG investigation; GAO forensic audit or special investigation; sustained national media coverage; industry/public backlash and decrease in confidence.	Director is replaced and senior staff is replaced (Mission impacts between one-hundredth to up to one-tenth of the Deepwater Hori*zon* impacts)
Low	10 to 100 deaths	20,000 to 100,000 bbls of crude oil released	$100 Million to $1 Billion	GAO, Congressional, and White House inquiries; sustained regional media coverage; unfavorable industry/public response.	Senior staff is replaced and some internal reorganization occurs (Mission impacts between one-thousandth to up to one-hundredth of the Deepwater Horizon impacts)
Very Low	<10 deaths	1 to 20,000 bbls of crude oil released	<$100 Million	Limited Congressional and departmental inquiries; short-term regional media coverage; industry/public concern.	Needing minor organizational or management system adjustments to accomplish mission (Mission impacts below one-thousandth of the Deepwater Horizon impacts [e.g., Black Elk])

Heat Map

In the figure below, the enterprise risk heat map is divided into five regions. Each color indicates regions of cells expecting similar responses to the risk exposure mapped in that region. Cell groupings are based on consecutive risk cell numbers, which increase with importance. Events with higher severity generally require a more significant risk response. For example, the risk cell with Very High Likelihood and Very Low Severity (cell 11) is colored yellow while the risk cell with Very Low Likelihood and Very High Severity (15) is colored orange.



SEVERITY

LIKELIHOOD

	Very Low	Low	Medium	High	Very High
Very High	11	16	20	23	25
High	7	12	17	21	24
Medium	4	8	13	18	22
Low	2	5	9	14	19
Very Low	1	3	6	10	15

Each color region on the risk heat map reflects a different degree of risk tolerance to a strategic risk falling in that region and consequently the suggested need for response. The following paragraphs provide brief descriptions of notional responses when an assessed strategic risk falls in a particular risk region.

- DARK RED (Risk Region V or Very High): Any risk in this zone substantially exceeds both the program's risk tolerance and risk appetite. All risks must be reduced by additional/modified risk treatments or must be approved by program leadership and communicated to the agency.
- RED (Risk Region IV or High): Any risk in this zone exceeds both program's risk tolerance and risk appetite. All risks must be reduced by additional/modified risk treatments or must be approved by program leadership and communicated to the agency.
- ORANGE (Risk Region III or Medium): While a risk is within the [AGENCY]'s risk tolerance in this zone, more than some agreed-upon number of strategic risks in this zone would exceed [AGENCY]'s risk appetite and the number of strategic risks falling in the zone must either be reduced or approved by program leadership and communicated to the agency.
- YELLOW (Risk Region II or Low): While risks within this zone are within [AGENCY]'s risk tolerance and risk appetite, additional risk treatments may still provide sufficient risk-reward to justify implementation.

- GREEN (Risk Region I or Very Low): Risks within this zone are within [AGENCY]'s risk tolerance and risk appetite and are not expected to require any additional risk treatments.

Strategic risks with assessed risk levels exceeding [AGENCY]'s risk tolerance require additional risk treatments. A key benefit in performing ERM is the collective management of risk treatments across all enterprise risks. With the risks and associated confidence assessed, specific risk treatments will be proposed for each strategic risk category. [AGENCY] leadership may then pursue the balance between the most efficient and effective risk treatments across all strategic risk categories.

d. Example #4

Risk Significance refers to the magnitude, potential impact or effect of a specific risk. Significance is rated on a numerical scale of 1 to 5.

Extreme (Rating-5) – Risks that are likely to have critical impact on the agency and/or the business unit in that order. Extreme risks are potentially business ending events, or at the very least could prevent the business unit from accomplishing its mission, not just a single goal or objective. Extreme risks have significant potential for grave consequences on an organization, its people, and /or processes. Very few risks fall in to this rating category, and many business units will not have any such risks.

Major (Rating-4) – Risks that are likely to have substantial impact on the agency, the business unit and/or area, in that order. Major risks can significantly hamper an organization's ability to achieve multiple and/or key goals and objectives. They also could rise to the level or preventing or impairing an organization from achieving its mission. Major risks often have serious internal and/or external repercussions. This is often the top rating category in terms of significance for the majority of business units. Usually, only a small percentage of risks fall into this category.

Significant (Rating-3) – Risks that have the potential to have considerable impact on the business unit and/or area. Significant risks can affect the achievement of one or more goals and objectives, but usually will not rise to the level of preventing an organization from achieving its mission. Significant risks may have substantial internal and/or external repercussions. A large percentage of risks fall into this rating category.

Moderate (Rating-2) – Risks that may have discernable impact on the business unit and/or area. Moderate risks can hamper the ability of a business unit or area to achieve one or more objectives, usually those of lesser significance. Occasionally they will rise to the level where they could actually prevent the achievement of a business unit's goals or objectives, but are unlikely to have any impact on the business unit's ability to achieve its mission. Many risks fall into this rating category.

Minor (Rating-1) – Risks that have little or no impact on the business unit and/or area. Minor risks can hamper the ability of a business unit or area to achieve a goal or objective, usually one of lesser significance. Rarely will they rise to the level where they could actually prevent the business unit or area from achieving a goal or objective. They do not have any discernable impact on the business unit's ability to achieve its mission. Usually, only a small percentage of risks fall into this category.

Risk Likelihood is the probability of the occurrence of a specific risk event. Risk likelihood is also rated on a numerical scale of 1 to 5.

Likelihood scores are based on empirical evidence and are discussed with key accountable parties. Scores are updated to reflect changes in the environment or status. Likelihood scores are based on a scale of 1-5 with 5 being the highest likelihood rating. Definitions for the risk scores are listed below:

Risk Scores		Definition	Likelihood Percentage (%)	Treatment of Issues / Level of Action
1	Very Remote	A risk that has little to no chance to occur. A risk that has very robust and / or long-standing mitigation and / or management strategies in place.	0 – 10	Key accountable parties monitor these risks and escalate issues if / when they arise. As mitigants / strategies are usually in place, these risks require less intensive monitoring.
2	Unlikely	A risk that is not likely to occur. A risk that has strong mitigation and /or management strategies in place that are functioning as intended.	10 - 35	Key accountable parties monitor these risks and escalate issues if / when they arise. RM works with key accountable parties on an intermittent basis.
3	Possible	A risk that has a chance to occur. Mitigation and / or management strategies are in place but may not be robust enough to prevent the risk from occurring. However, the mitigation / management strategies in place would most likely lessen the chance of occurrence.	35 - 65	Reasonably certain that some level of mitigation or management strategies exist. RM works with accountable parties on an "as-needed" basis.
4	Probable	A risk that is more likely to occur than not to occur; a high degree of certainly that the risk will occur. A risk that has more than a 50% chance of occurring. Effective mitigation and /or management strategies are not in place or are not functioning as intended.	65 - 90	RM works with key accountable parties on a regular basis to ensure mitigation and management strategies exist.
5	Very Likely	A risk that is occurring or is certain to occur given the environment or factors involved. Mitigation and /or management strategies are not in place or are not functioning as intended.	90 - 100	RM works aggressively with key accountable parties to ensure mitigation and management strategies exist.

Significance					
5	🟩 5	🟧 10	🟧 15	🟥 20	🟥 25
4	🟩 4	🟨 8	🟧 12	🟥 16	🟥 20
3	🟦 3	🟨 6	🟨 9	🟧 12	🟧 15
2	🟦 2	🟩 4	🟨 6	🟨 8	🟧 10
1	🟦 1	🟦 2	🟦 3	🟩 4	🟩 5
	1	2	3	4	5

Likelihood

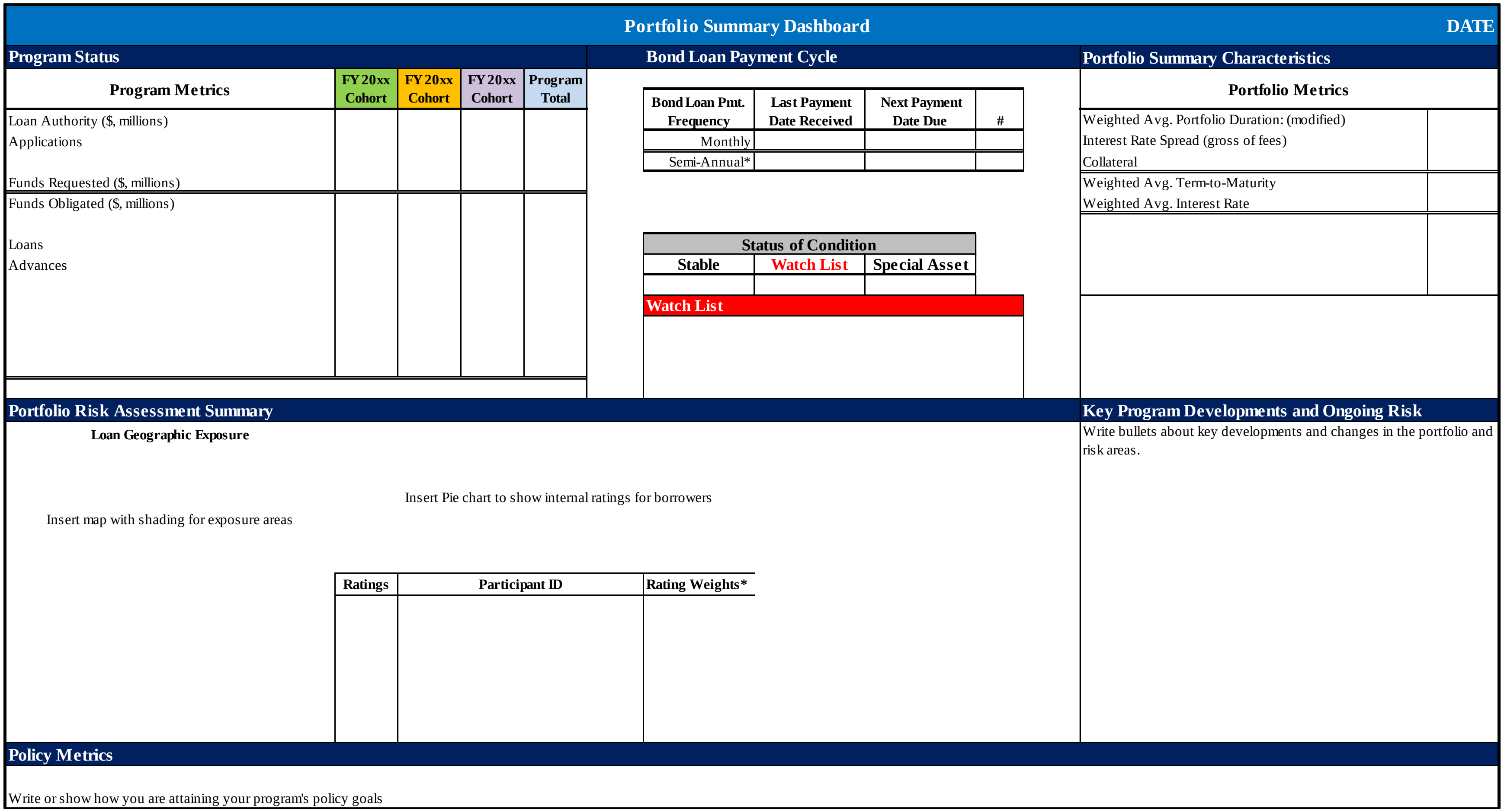
Aggregate Risk Scores[11]

Critical (20-25)	-	🟥
High (12-16)	-	🟧
Medium (6-10)	-	🟨
Moderate (4-5)	-	🟩
Low (1-3)	-	🟦

[11] Cumulative risk scores are calculated by multiplying the significance and likelihood ratings of a particular risk.

E. Risk Reporting and Monitoring

1. Dashboards[12]



Portfolio Summary Dashboard DATE

Program Status

Program Metrics	FY 20xx Cohort	FY 20xx Cohort	FY 20xx Cohort	Program Total
Loan Authority ($, millions)				
Applications				
Funds Requested ($, millions)				
Funds Obligated ($, millions)				
Loans				
Advances				

Bond Loan Payment Cycle

Bond Loan Pmt. Frequency	Last Payment Date Received	Next Payment Date Due	#
Monthly			
Semi-Annual*			

Status of Condition		
Stable	Watch List	Special Asset

Watch List

Portfolio Summary Characteristics

Portfolio Metrics	
Weighted Avg. Portfolio Duration: (modified)	
Interest Rate Spread (gross of fees)	
Collateral	
Weighted Avg. Term-to-Maturity	
Weighted Avg. Interest Rate	

Portfolio Risk Assessment Summary

Loan Geographic Exposure

Insert map with shading for exposure areas

Insert Pie chart to show internal ratings for borrowers

Ratings	Participant ID	Rating Weights*

Key Program Developments and Ongoing Risk

Write bullets about key developments and changes in the portfolio and risk areas.

Policy Metrics

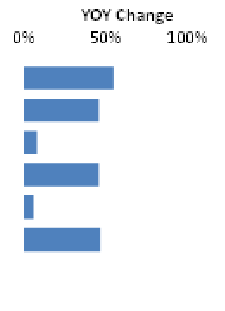
Write or show how you are attaining your program's policy goals

[12] Please see OMB Circular A-129 Appendix D for many examples of dashboards that include risk analysis. https://www.whitehouse.gov/sites/default/files/omb/assets/a129/rev_2013/pdf/a-129.pdf

Grant Program Dashboard
As of DATE

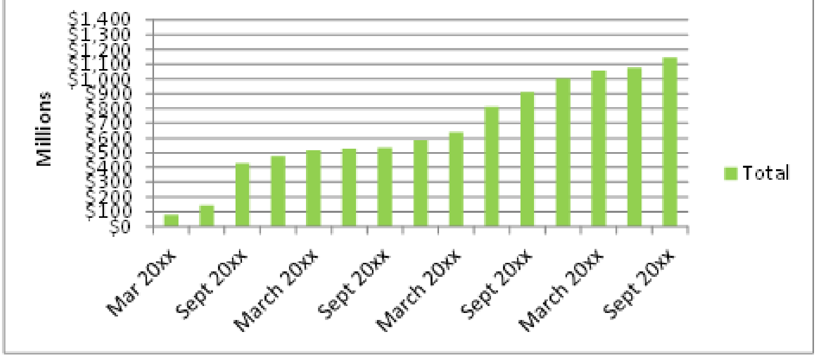
Allocated and Deployed Funds		% of Total Allocated Funds
Allocated Funds	$	
Total Funds Deployed	$	%
Original Deployed	*$*	%
Recycled Funds Deployed	*$*	%

Portfolio Summary		
	12/31/20xx	12/31/20xx
Total Private Financing (cumulative)	$	$
AGENCY Dollars Expended (cumulative)	$	$
Private Leverage (cumulative)		
No. of Investments (cumulative)		
Avg. Total Private Financing	$	$
Jobs Created & Retained (cumulative)		



Disbursements					% of Total Allocated Funds
	Quarter	Number of Disbursements	Amount	Total Disbursed	
Actual	3Qxx	0	$0	$0	%
Projected	4Qxx	0	$0	$0	%
Projected	1Qxx	0	$0	$0	%
Projected	2Qxx	0	$0	$0	%
Projected	3Qxx	0	$0	$0	%

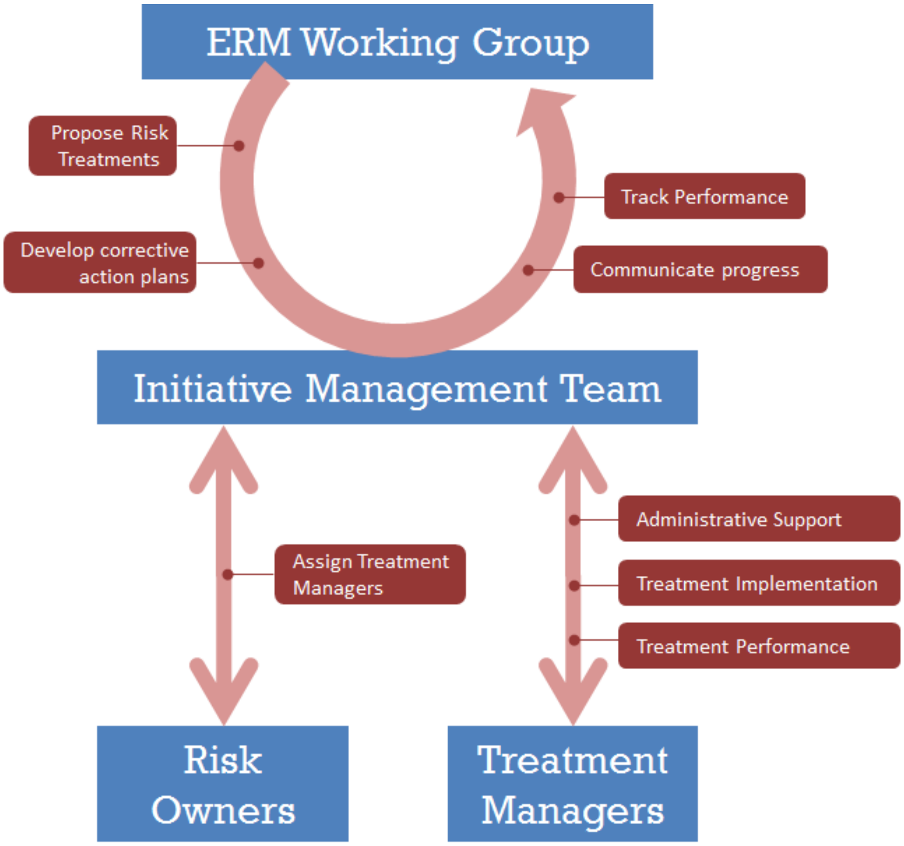
Disbursements of Funds
(Cumulative through September 30, 20xx)



2. Monitoring

a. Risk Monitoring and Governance for Communicating Risk (Example)

The Initiative Management Team (IMT) serves the function of initiating, facilitating, monitoring, and evaluating the performance of projects across an organization. In the context of risk treatments, each treatment selected for implementation is treated as a project. The project is assigned to an individual who takes the lead on its implementation and is held accountable for its success (i.e., Treatment Manager). The project lead can access the IMT for administrative support and the IMT should periodically contact the project lead for updates and progress reports. If over the course of the project there is an issue identified by the IMT in the management of the project, the IMT should work with the project lead to identify recommended actions to get the project on track.



The IMT would serve as a centralized and consolidated point of contact for all project progress and delivery performance. Leadership would engage with the IMT to identify project leads, track project progress, and review implementation effectiveness. This model facilitates efficient flow of information and removes the burden on leadership to collect information from individual project managers, instead providing a single source of data. Through the IMT, leadership can track the progress of treatment implementation and develop corrective action plans if necessary.

The IMT would consist of the Chief Risk Officer, Performance Management Office representatives, and administrative staff. The IMT Roles and Communication Figure shows how the IMT interacts with other participants in the ERM process.

b. *Risk Monitoring Treatment Template (Example)*

Risk Title:				Risk Manager:	
Treatment Plan Summary:					
Treatment Plan Status:					Risk Trend:
Task No:	Task Description	Action Owner	Estimated Completion Date	Actual Completion Date	Resulting L,C
1					
2					
3					
4					
Contingency Plan:					Trigger:
Treatment Alternatives Considered					

F. Glossary

Term	Definition
A-123	Refers to OMB Circular No. A-123, which defines management's responsibility for enterprise risk management and internal control in Federal agencies.
Acceptance	Risk response where no action is taken to respond to the risk based on the insignificance of the risk; or the risk is knowingly assumed to seize an opportunity.
Aggregate Risk	The total or cumulative amount of exposure associated with a specified risk. Aggregate risk is comprised of two components: significance and likelihood, and does not include the effect of risk strategies, controls or other measures in place to designed to mitigate the effect or reduce exposure to the specified risk.
Application Controls	Programmed procedures in application software, and related manual procedures, designed to help ensure the completeness and accuracy of information processing.
Avoidance	Risk response where action is taken to stop the operational process, or the part of the operational process causing the risk.
Capital	General term which refers to financial assets, the financial value of assets such as cash, or other financial resources available for use by an organization.
Compliance Risk	Risk of failing to comply with applicable laws and regulations and the risk of failing to detect and report activities that are not compliant with statutory, regulatory, or organizational requirements. Compliance risk can be caused by a lack of awareness or ignorance of the pertinence of applicable statutes and regulations to operations and practices.
Computer Controls	Controls performed by a computer, i.e., controls programmed into computer software, and controls over the automated processing of information, consisting of general controls and applications controls.
Control Activities	The policies and procedures that help ensure management directives are effectively carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties.
Control Self-Assessment	A process through which internal control effectiveness is examined and assessed. The objective is to provide reasonable assurance that all business objectives will be met.
Controls	Policies or procedures that are part of a system of internal control.

Term	Definition
Corporate Governance	The set of processes, customs, policies, laws and regulations affecting the way an organization is directed, administered, or controlled.
COSO	Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting. COSO was jointly sponsored by five organizations: the American Accounting Association, American Institute of CPA's, Financial Executives International, Institute of Internal Auditing and the Institute of Management Accounting. In 1992, COSO issued a landmark report on internal control: *Internal Control—Integrated Framework*, which provides for establishing internal control systems and evaluating their effectiveness. In September 2004, COSO released *Enterprise Risk Management - Integrated Framework*, which provides guidance and standards for implementing ERM.
Cost/Benefit Analysis	A technique designed to determine the feasibility of a project or plan by quantifying its costs and benefits.
Credit Program Risk	The potential that a borrower or financial counterparty will fail to meet its obligations in accordance with their terms. If the credit exists in the form of a direct loan or loan guarantee, credit risk is the risk that the borrower will not fully repay the debt and interest on time.
Cyber Information Security Risk	Risk that could expose the agency to exploitation of vulnerabilities to compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by its information systems.
Enterprise Risk Management (ERM)	An effective agency-wide approach to addressing the full spectrum of the organization's significant risks by considering the combined array of risks as an interrelated portfolio, rather than addressing risks only within silos. ERM provides an enterprise-wide, strategically-aligned portfolio view of organizational challenges that provides improved insight about how to more effectively prioritize and manage risks to mission delivery.
Entity	An organization established for a particular purpose (e.g. a corporation, government body, academic institution, etc.) Synonyms include organization and enterprise.
Event	An incident or occurrence, from sources internal or external to an entity that affects achievement of objectives.
Financial Risk	Risk that could result in a negative impact to the agency (waste or loss of funds/assets).
Financial Risk Management	The practice of creating value in an organization by using financial instruments or models to manage exposure to risk.
Fraud	Dishonesty in the form of an intentional deception or a willful misrepresentation of a material fact.

Term	Definition
General Controls	Policies and procedures that help ensure the continued, proper operation of computer information systems. They include controls over information technology (IT), IT infrastructure, security management, and software acquisition, development and maintenance.
Government Performance and Results Act Modernization Act (GPRAMA)	Requires that agencies revise strategic plans every four years, and assess progress toward strategic objectives annually.
Impact	The effect of an event on strategic goals and objectives. Impact can be positive or negative related to the organization’s objectives.
Inherent Risk	The exposure arising from a specific risk before any action has been taken to manage it beyond normal operations. Inherent risk is often referred to as “the risk of doing business”.
Integrity	The quality or state of being of sound moral principle, honest and sincere. The desire to do the right thing, to profess and live up to a set of values and expectations.
Interest Rate Risk	The risk associated with fluctuations in interest rates and the impact on investments, loans or business activities.
Internal Control	A process, affected by an organization's management or other personnel, designed to provide reasonable assurance regarding the achievement of objectives.
Internal Control Environment	The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility, and organizes and develops its people; and the attention and direction provided by the board of directors.
IT Controls	Refers to the broad category of information technology controls including computer, application, and general controls.
Key Performance Indicator	Key Performance Indicators (KPIs) are financial and nonfinancial metrics used to monitor changes in business performance in relation to specific business objectives (e.g. volumes of business, revenue etc.).
Key Risk Indicator	Key Risk Indicators (KRI's) relate to a specific risk and demonstrate a change in the likelihood or impact of the risk event occurring.
Legal Risk	Risk associated with legal or regulatory actions and agency’s capacity to consummate important transactions, enforce contractual agreements, or meet compliance and ethical requirements.
Legislative Risk	Risk that legislation could significantly alter the mission (funding, customer base, level of resources, services, and products) of the agency.

Term	Definition
Likelihood	The probability that a given event will occur.
Liquidity Risk	Risk that an organization will not have sufficient funds available to settle one or more financial obligations for full value when they become due (even if the organization may be able to settle that obligation at some unspecified time in the future).
Management Controls	The organization, policies, and procedures used by agencies to reasonably ensure that (i) programs achieve their intended results; (ii) resources are used consistent with agency mission; (iii) programs and resources are protected from waste, fraud, and mismanagement; (iv) laws and regulations are followed; and (v) reliable and timely information is obtained, maintained, reported and used for decision making.
Management Fraud	The intentional misrepresentation of corporate or unit performance levels perpetrated by employees serving in management roles who seek to benefit from such frauds in terms of promotions, bonuses or other economic incentives, and status symbols.
Manual Controls	Refers to controls performed manually, not by computer or some other automated means.
Objective Setting	One of the eight components of ERM. Objective setting involves establishing desired objectives (goals) to complete within a specified period of time. Objective setting occurs at all levels of an organization. Objectives set at the strategic level, help establish a basis for operations, reporting and compliance. Objective setting is a precondition to other ERM components including event identification, risk assessment and risk response.
Occupational Fraud	The use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization’s resources or assets.
Operational Risk	The risk of direct or indirect loss arising from inadequate or failed internal processes, people and systems, or external events. It can cause financial loss, reputational loss, loss of competitive position or regulatory sanctions.
Opportunity	A favorable or positive event. In context of risk management, it refers to the possibility that an event will occur and positively affect the achievement of objectives.
Political Risk	Risk that may arise due to actions taken by Congress, the Executive Branch or other key policy makers that could potentially impact business operations, the achievement of the agency's strategic and tactical objectives, or existing statutory and regulatory authorities. Examples include debt ceiling impasses, government closures, etc.
Probability	A quantitative measure indicating the possibility that a given event will occur. Probability is usually indicated in terms of a percentage, frequency of occurrence, or other numerical metric.
Reduction	Risk response where action is taken to reduce the likelihood or impact of the risk.

Term	Definition
Regulatory Risk	The risk of problems arising from new or existing regulations. Such problems may include: changes in laws or regulations having significant impact on the organization, an inability for an organization to establish the right policies and procedures to be in compliance with regulations, or an increase in the cost and complexity to ensure compliance with new and existing regulations.
Reporting Risk	The risk associated with the accuracy and timeliness of information needed within the organization to support decision making and performance evaluation, as well as, outside the organization to meet standards, regulations, and stakeholder expectations. This is a subset of operational risk.
Reputational Risk	Risk that a failure to manage risk, external events, and external media or to fail to fulfill the agency's role (whether such failure is accurate or perceived) could diminish the stature, credibility or effectiveness of the agency. Reputational risk can arise either from actions taken by the agency or third party partners including service providers and agents. Reputational Risk can also arise from negative events in one of the other risk categories such as Legal and Compliance risks.
Residual Risk	The amount of risk left over after action has been taken to manage it, (such as establishing internal controls).
Review (Verification and Validation)	The process by which assessment of risks is evaluated by senior management.
Risk	The effect of uncertainty on achievement of objectives. An effect is a deviation from the desired outcome – which may present positive or negative results.
Risk Action Plan (RAP)	A set of actions designed to mitigate or exploit identified risks. The plan may include intended outcomes and timetables and any other follow-up work necessary.
Risk Appetite	The articulation of the amount of risk (on a broad/macro level) an organization is willing to accept in pursuit of strategic objectives and value to the enterprise.
Risk Assessment	The identification and analysis of risks to the achievement of business objectives. It forms a basis for determining how risks should be managed. Risk assessment involves evaluating the significance and likelihood of a risk, as well as any controls or other measures that mitigate or eliminate that risk.
Risk Assessment Score	A weighting of a potential outcome (positive/negative) multiplied by probability of its occurrence and used to prioritize choices.
Risk Impact	A measurement of the effect that could result from the occurrence of a particular identified risk.
Risk Management	A coordinated activity to direct and control challenges or threats to achieving an organization's goals and objectives.

Term	Definition
Risk Mitigation	Strategy for managing risk that seeks to lower or reduce the significance and/or likelihood of a given risk.
Risk Profile	A prioritized inventory of an organization’s most significant risks.
Risk Response	Management's strategy for managing (or responding to) a given risk. Risk response strategies include: avoidance, sharing, reduction, transfer and acceptance.
Risk Strategy	Synonymous with risk response. The strategy for managing (or responding to) a given risk. Risk response strategies include: avoidance, sharing, reduction, transfer and acceptance.
Risk Tolerance	The acceptable level of variance in performance relative to the achievement of objectives.
Sharing	Risk response where action is taken to transfer or share risks across the organization or with external parties, such as insuring against losses.
Significance	Magnitude or potential impact of a specified risk.
Strategic Risk	Risk that would prevent an area from accomplishing its objectives (meeting the mission).
Technology Risk	The broad risk associated with computers, e-commerce, and on-line technology. Examples of technology risks include: network/server failures, obsolescence, lack of IT resources and skills, loss/theft of client/customer data, inadequate system security, viruses, denial of service, systems availability, and integration issues.
Uncertainty	The inability to know in advance the exact likelihood or impact of future events.
Value at Risk (VaR)	Measure of how the market value of an asset or of a portfolio of assets is likely to decrease over a certain time period under usual conditions. It is typically used by security houses or investment banks to measure the market risk of their asset portfolios (market value at risk), but is actually a very broad concept that has broad application.

G. References and Resources

Title/Description	Source
"How-To" Tutorial Coordinating ERM Implementation Planning in a Federated Agency	http://business.gmu.edu/images/contentattachments/FERM2015_BringingERMtotheSystem_1.pdf
AFERM Training	https://www.aferm.org/
Committee of Sponsoring Organizations of the Treadway Commission (COSO)	http://www.coso.org/
GAO Fraud Book	http://www.gao.gov/products/GAO-15-593SP
Green Book	http://www.gao.gov/greenbook/overview
North Carolina State University Thought Paper "Reporting Key Risk Information to the Board of Directors"	https://erm.ncsu.edu/az/erm/i/chan/library/2015-erm-reporting-key-risk-information-to-board-directors.pdf
RIMS	https://www.rims.org/Pages/Default.aspx
RMA Risk Appraisal Workbook	http://www.rmahq.org/enterprise-risk-management-workbooks/
UK Orange Book	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf

H. Agency Acknowledgements

The Chief Financial Officers Council and Performance Improvement Council would like to thank the following individuals for their contributions to the Playbook:

Steering Committee

Name	Agency
Carol Bales	Office of Management and Budget (OMB)
Mark Bussow	OMB
Lilly Gilmour	General Services Administration (GSA)
Gary Grippo	U.S. Department of the Treasury (Treasury)
Karen Hardy	Department of Commerce (Commerce)
Jeff Johnson	Department of Health and Human Services (HHS)
Justin Johnson	Office of Personnel Management (OPM)
Christine Jones	HHS
Dan Kaneshiro	OMB
Regina Kearney	OMB
Michael Landry	OMB
Adam Lipton	OMB
Ken Phelan	Treasury
Mary Reding	GSA
Dana Roberts	GSA
David Rowe	OMB
Curtina Smith	OMB
Cynthia Vitters	Department of Education (Education)
Mike Wetklow	National Science Foundation (NSF)

Working Group

Name	Agency
John Ascienzo	U.S. International Trade Commission (USITC)
Jessie Bailey	OMB
Eduardo Barcelo	HHS
Cory Baumhardt	Department of Transportation
Anju Bhargava	Social Security Administration
Greg Blaszko	OPM
Amy Borgstrom	Corporation for National and Community Service
Jamal Bouaichi	U.S. Department of Housing and Urban Development (HUD)

Name	Agency
Susan Bowers	National Nuclear Security Administration
Vicky Cabrera	Treasury
Catherine Chatfield	HHS
David Coontz	National Archives and Records Administration
Hilary Cronin	Education
Kelly Cummins	Department of Energy (Energy)
Mark Daley	Commerce
Lisa Davis	HHS
Carolyn Dempster	Education
Rodney Dixon	HHS
Tonya Dunham	Consumer Financial Protection Bureau (CFPB)
Claude Etienne	U.S. Securities Exchange Commission
Carol Eyerman	NSF
Andrea Fisher - Colwill	Treasury
Daniel Fodera	Federal Highway Administration
Cassandra Freeman	HHS
Silvia Galluch	USITC
Melissa Giambi	Education
Lori Giblin	Corporation for National and Community Service
Zoya Kaplan	Department of Labor
Cheh Kim	Federal Deposit Insurance Corporation (FDIC)
Christopher Landers	Energy
Jacob Lee	Bureau of Safety and Environmental Enforcement
Francisco Lepe	HHS
Linda Linkins	USITC
Javier Lopez	HHS
Sarah Lyberg	HUD
Lisa Maguire	HUD
Colleen McLoughlin	Treasury
Thomas Moschetto	OPM
Ralph Newsome	Energy
Sabrina Nolasco	CFPB
Frances Nwachuku	Energy
Jill Oliver	FDIC
John Rich	GSA
Neil Ryder	Department of Justice (Justice)
Katy Sartorius	Energy

Name	Agency
Jason Stayanovich	HUD
Meredith Stein	National Institutes of Health
Katherine Tkac	Smithsonian
Karen Weber	Treasury
Douglas Webster	U.S. Agency for International Development
Debra Williams	Justice
Diana Woodfolk	HHS
Katie Wurtz-Brodfuehrer	Federal Trade Commission
Montrice Yakimov	Bureau of the Fiscal Service
Andy Zino	Smithsonian