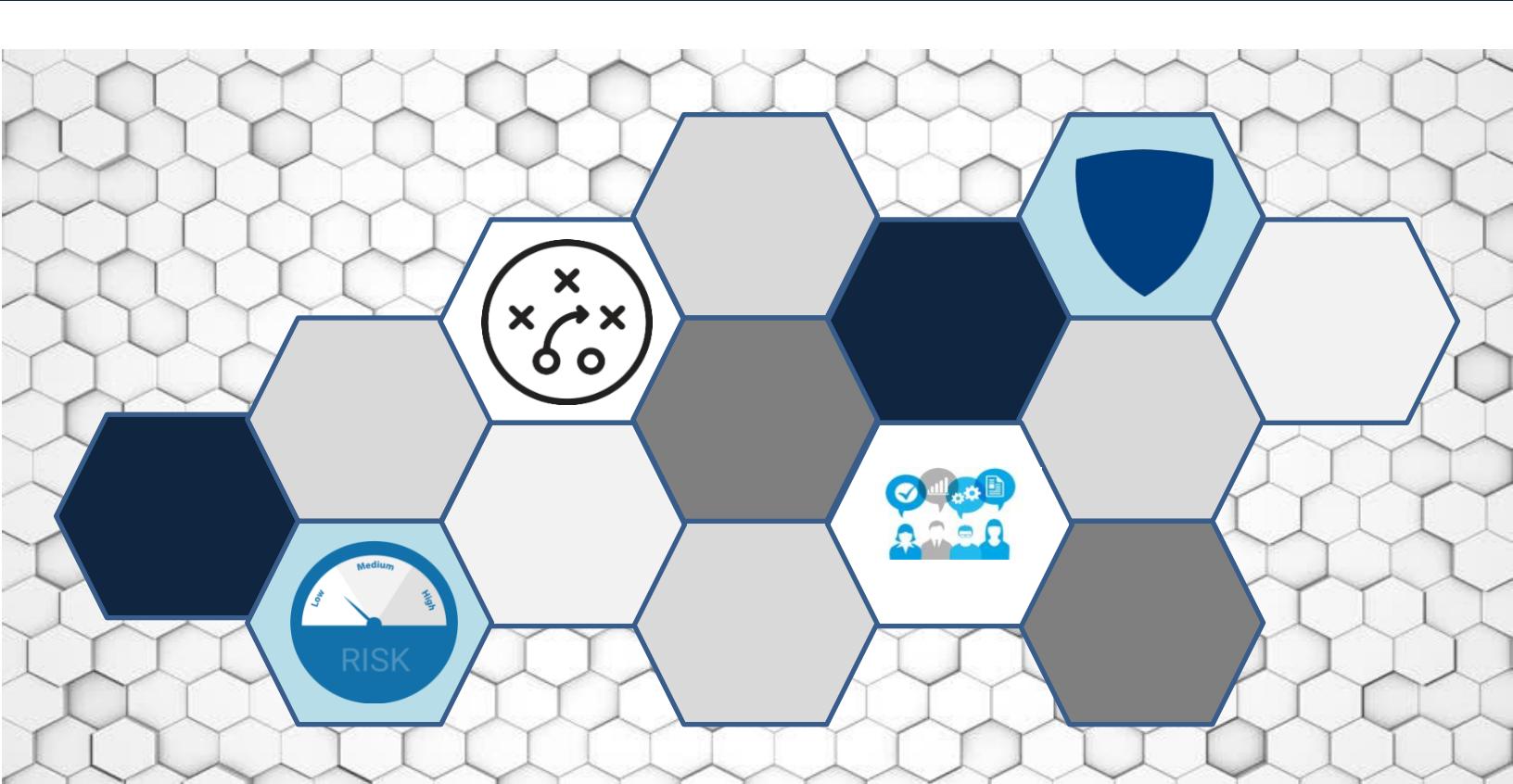


# Playbook:

## Enterprise Risk Management

### for the U.S. Federal Government

(Fall, 2022 Update)



*Developed and issued in collaboration with Federal Government organizations  
to provide guidance and support for Enterprise Risk Management.*

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



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

DATE: November 28, 2022

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

As our experience these past two years responding to the COVID-19 pandemic illustrates, integrating sound risk management approaches and practices at both the programmatic as well as enterprise level into agency management routines is critical for effective operational and strategic planning. Thus, the Chief Financial Officers Council (CFOC) and the Performance Improvement Council (PIC) are releasing this update to the *Playbook: Enterprise Risk Management (ERM) for the U.S. Federal Government* (Playbook) as an inter-council effort convened by the Office of Shared Solutions and Performance Improvement of the General Services Administration. Led by agencies, the updated Playbook resulted from the efforts of a Working Group of ERM practitioners who are members of the ERM Community of Practice from over 50 federal agencies and included cross-functional representation.

The updated Playbook contains expanded sections on incorporating ERM into management practices, risk appetite and tolerance, workforce, a new section on ERM and Cybersecurity, and updated appendices, including a new ERM maturity model.

Because the Playbook was always intended to be updated as agencies' ERM capabilities mature, future revisions to the Playbook will be released as this critical management function evolves to provide support to agency leadership decision-making. As part of these ongoing efforts, we will continue to accept comments, suggestions, and examples for the Playbook through the CFO and PIO Councils and ERM Community of Practice.

# Table of Contents

I. Introduction .....	4
A. Using This Playbook .....	4
B. What is Risk Management? What is ERM? Why Do Government Agencies Need Them? .....	5
C. Integrating ERM into Government Management Practices .....	6
II. Enterprise Risk Management Basics.....	17
A. Outcomes and Attributes of Enterprise Risk Management .....	17
B. Common Risk Categories.....	17
C. Principles of Enterprise Risk Management.....	18
D. Maturity of ERM Implementation.....	20
III. ERM Model .....	20
IV. Developing an ERM Implementation Approach.....	25
V. Risk Governance .....	26
A. Culture and Governance.....	26
B. Organizational Design, Alignment, Leadership and Staffing .....	27
VI. The Risk Appetite Statement.....	28
A. What is Risk Appetite and Risk Tolerance? .....	28
B. Methods for Assessing and Updating Risk Appetite.....	30
C. Methods for Establishing a Risk Appetite Statement.....	33
D. Considerations When Developing Risk Appetite .....	34
E. Examples of Risk Appetite being applied in an agency .....	35
VII. Developing a Risk Profile .....	38
A. Steps to Creating a Risk Profile .....	38
B. Additional Considerations .....	47
VIII. GAO/OIG Engagement.....	48
IX. Special Chapter: Integration of Agency ERM with Information Security and Cybersecurity Risk Management.....	48
A. Foundations of Information Security and Cybersecurity .....	48
B. ERM Principles within Information Systems.....	52
C. Approaches to ERM, Information Security, and Cybersecurity Risk Management Integration.....	56
D. Addressing Confusion in FISMA Audits.....	59
X. Appendices .....	61

# 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 Office of Management and Budget (OMB) Circular No. A-123 (OMB A-123). The appendices are 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. This shared knowledge will 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. A useful tool for those throughout an organization to improve decision-making, strategy, objective-setting, and daily operations;
4. Practical support for operational level staff who manage day-to-day risks in the delivery of the organization's objectives;
5. A reference for those who review risk management practices, such as those serving on Risk Committees; and
6. Helpful for implementing the requirements of OMB Circulars A-11 and A-123.<sup>1</sup>

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 program, 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

---

<sup>1</sup> Note that OMB Circulars A-11 and A-123 does not seek to describe a comprehensive ERM program, and the requirements set forth are not required for all agencies but are required for CFO Act agencies.

management activities already underway and encompass an agency's key operations.

Responsibility for managing risks is shared throughout the agency from the highest levels of executive leadership to the service delivery staff. 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 Circulars A-11, A-123 or other guidance. While this Playbook provides the foundation for applying ERM principles and meeting the requirements of the Circulars, 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 a 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 agencies make better-informed decisions based on a holistic view of risks and their interdependencies. The appendices include examples of documents some agencies have found helpful.

This document is not intended to set standards for audit or other compliance reviews, nor is it intended to be prescriptive.

## **B. What is Risk Management? What is Enterprise Risk Management? 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 beneficial to the public interest, especially in areas where the private sector is either unable or unwilling to do so. This work is surrounded by uncertainty, posing threats to successfully achieving objectives while at the same time offering opportunities to increase value to the American people through planning and mitigation.

While agencies cannot respond to all risks, one of the most salient lessons learned from past crises and negative reputational incidents is that public and private sector organizations both 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 and opportunities related to mission delivery and manage risk within their established tolerances and appetites.

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 and opportunities as an interrelated portfolio, rather than addressing risks only within silos. ERM provides an enterprise-wide, strategically-aligned portfolio view of organizational challenges and opportunities that provide improved insight to more effectively prioritize and manage risks to mission delivery.<sup>2</sup>

Effective ERM facilitates improved decision-making through a structured understanding of opportunities and threats. Effective ERM also helps agencies implement strategies to use resources effectively, optimize approaches to identify and remediate compliance issues, and promote reliable reporting and monitoring across business units. It promotes a culture of better understanding, disclosure, and

---

<sup>2</sup> OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget, Section 260*.

management of agency risks and opportunities. The benefits of ERM integration include the ability to: increase opportunities, increase positive outcomes and advantages, reduce negative surprises, identify and manage entity-wide risks, reduce performance variability, and improve resource deployment.<sup>3</sup> ERM 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 ensure risks are managed effectively, efficiently, and coherently across an agency.

An ERM framework allows Federal departments and agencies to increase risk awareness and transparency, improve risk management strategies, and align risk taking to each agency's risk appetite and risk tolerance. **Risk Appetite** is 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.<sup>4</sup> **Risk Tolerance** is the acceptable level of variance in performance relative to the achievement of objectives.<sup>5</sup> 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 for accepting, reducing, sharing, pursuing, or avoiding risk that ultimately results in more resilient, effective, and efficient government programs. ERM can help to focus and strengthen decisions by informing the development of goals and objectives and the strategies to achieve them. This includes advocating for and aligning resources, monitoring progress, and ensuring compliance with applicable laws, regulations, and controls.

---

### ERM Pitfall ERM not integrated

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

---

Integrating ERM into agencies' decision-making and management practices can be done successfully and in various ways. It can be supported by co-locating the ERM function with other management functions such as strategic planning, organizational performance, budget, or internal controls; through the ERM function and other management functions reporting to the same management official; or through equal organizations with strong collaboration across the offices. While there is no one-size-fits-all approach to organize an ERM program to achieve integration, it is imperative that the ERM function be tailored to the function, characteristics, and culture of the agency.

---

<sup>3</sup> The Committee of Sponsoring Organization of the Treadway Commission (COSO) *Enterprise Risk Management-Integrated Framework*, pgs. 6-7.

<sup>4</sup>The Committee of Sponsoring Organization of the Treadway Commission (COSO) *Enterprise Risk Management-Integrated Framework*, p. 20.

<sup>5</sup> Ibid.

OMB issued several guidance documents that call for the integration of ERM into existing management practices. For example, since the update to Circular A-123's release in 2016, enterprise risk management has been more fully incorporated into OMB Circular No. A-11 (OMB A-11). As shown in Figure 1, OMB A-11 calls for agencies to consider and prioritize risks across the enterprise as part of program and service delivery and implementation, operations support, organizational strategic and performance planning, and budget decisions and resource alignment (including the workforce). The updated Section 260 of OMB A-11 discusses agency responsibilities for identifying and managing strategic and programmatic risk as part of agency strategic planning, performance management, and performance reporting practices. The budget formulation sections of OMB A-11 state that agencies should include ERM as a basis for budget proposals.<sup>6</sup> OMB instructs that agencies, when creating their budget proposals, should use a comprehensive system that integrate analysis, performance management and strategic planning, evaluation, ERM, and budgeting, as well as appropriately incorporate the analyses and assessments resulting from the agency's annual strategic reviews.

Section II of OMB 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. It also requires agencies to develop "Risk Profiles" that identify major risks arising from mission and mission-support operations and analyze how those risks affect the agency's achievement of its strategic objectives. Appendix A of OMB A-123 was updated in 2018 and provides updated guidance to agencies that integrates internal control over reporting with ERM processes, and assurances over internal control. Specifically, the update expanded internal controls from financial reporting to all reporting objectives. By aligning the updated Appendix A to the agency's ERM processes, agency management should apply their analysis of risk in the agency's risk profiles across a portfolio view of the agency's objectives. They should decide where internal controls will be most effectively employed to those reporting objectives where inaccurate, unreliable, or outstanding reporting would significantly impact the agency's ability to accomplish its mission and performance goals or objectives. More importantly, management decisions to apply internal controls over reporting should not be done against the entire Annual Agency Performance Plan or Annual Agency Performance Report, but only where there is significant risk that a material reporting error may impact achievement of the agency's mission objectives and internal controls are likely to cost effectively mitigate the risk.

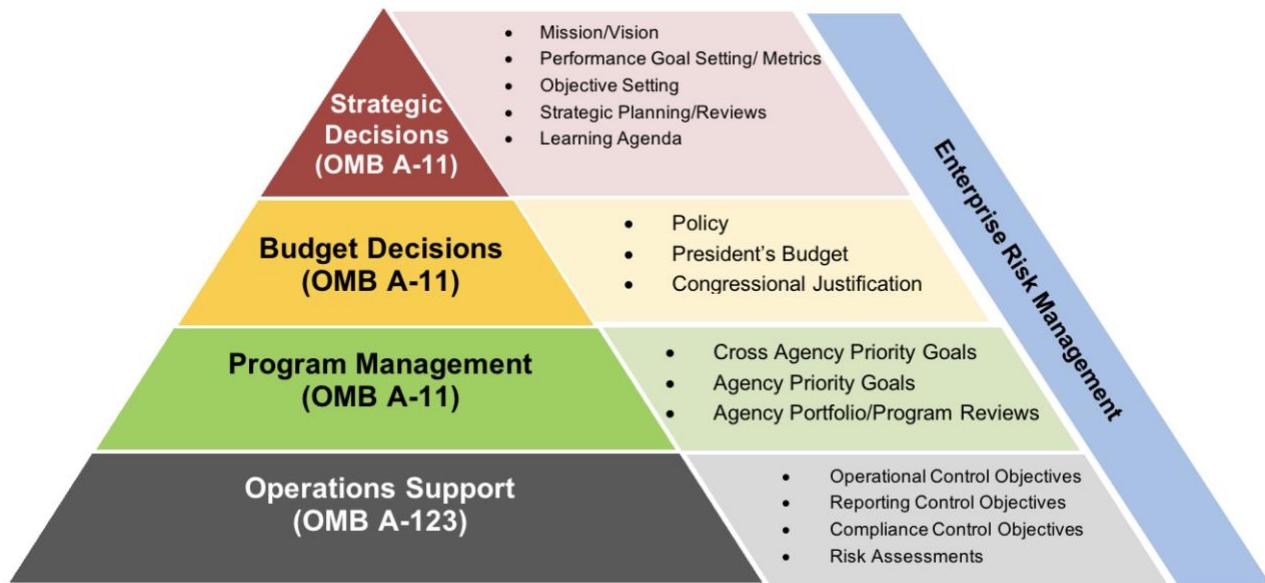
OMB A-123 and OMB A-11 constitute the core of the ERM policy framework for the Federal Government with specific ERM activities integrated and operationalized by Federal agencies.<sup>7</sup> The following figure shows the interplay among these two Circulars and controls, program management, budget, and strategic decisions within the ERM framework.

---

<sup>6</sup> See OMB Circular No. A-11, Section 51 and Part 6 (Sections 200-290).

<sup>7</sup> Requirements set forth in OMB A-11 and OMB A-123 are necessary for CFO Act agencies and are optional for others. Therefore, not everything discussed in this section may be relevant to all agencies.

**Figure 1: The ERM Policy Framework**



As shown in Figure 1, an effective ERM program is an integral part of the agency's decision-making processes. Agencies should 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 operational plans and implementation strategies, budgets, and the establishment of performance goals and controls.

In addition to the ERM guidance laid out in OMB A-11 and OMB A-123, OMB provides guidance on integrating risk management practices in the management of federal credit programs and non-tax receivables in OMB Circular No. A-129 (OMB 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 includes new sections on identifying, assessing, and responding to risks in the control environment.

In addition to issuing guidance on ERM, OMB demonstrated its commitment to ERM by establishing and chairing the ERM Executive Steering Committee. Membership includes representatives from several federal agencies.<sup>8</sup> Membership may change over time. Its mission is to promote and facilitate a risk-aware culture across the Federal Government by developing a Federal ERM framework and strategies; promote integrated strategy-setting with performance and cost management practices that are

---

<sup>8</sup> These agencies include the Department of Defense, Department of Justice, Department of the Treasury, Department of Veterans Affairs, Department of Health and Human Services, Consumer Financial Protection Bureau, Federal Deposit Insurance Corporation, and Small Business Administration.

supported by quality data agencies can rely on to manage risk in creating, preserving, and realizing value; and drive resource prioritization and allocation by leveraging risk-informed decisions across the Federal Government.

### **Integration with Strategic Planning and Performance Management**

Aligning strategic planning and performance management with ERM helps the agency understand possible risks to reaching its objectives and how to use risks to identify opportunities to meet those objectives. A goal of ERM is to strengthen an organization's capacity to manage risks by creating internal management processes that facilitate the identification of risks, resource allocation and alignment, and the proactive discussion of strategies and activities to manage negative risks and pursue positive risks and opportunities.

During the development of a Strategic Plan, it is important for agencies to identify and consider both negative and positive (opportunities) risks and articulate how they may evolve over time. Considering the future environment and its associated risks in the early stages of the strategic planning process will help the agency better align the management of risks with the organization's overall mission, goals, and objectives. When agencies develop their four-year Strategic Plans, they should leverage analytical processes and data, such as findings from annual strategic objective reviews, that assess progress being made against strategic objectives in the Agency Strategic Plan. Agencies should consider the top risks and opportunities to pursue based on strategies and objectives. These practices will help the agency identify the most effective long-term strategies.

As part of the strategic objective review process, agencies annually assess their progress toward achieving strategic goals and objectives. Through the evaluation of key performance indicators (KPIs), as well as other qualitative and quantitative success criteria, agencies can evaluate the effectiveness of their implementation strategies as identified in the agency's Strategic Plan and make changes accordingly while also identifying areas of noteworthy progress and focus areas for improvement. Through this lens, agency leadership can more effectively view the progress being made to improve program outcomes and look at opportunities for efficiencies. The annual reviews should leverage performance management, ERM, program management, and evaluation to determine where the agency has been (backward looking) and where the agency is going (forward looking). The results of these reviews, discussed with OMB during the Strategic Review meetings, helps inform decision-making processes, including possible effects of programmatic and operational risks on achieving strategic goals, objectives, and strategies. This organizational performance and management perspective facilitates the development of a learning-focused organization that successfully manages enterprise risks and opportunities.

Incorporating ERM into the strategic objective review process is critical and provides another lens by which agencies can more effectively identify opportunities and manage risks to performance, especially those risks related to achieving an agency's strategic objectives. An organizational view of risk allows the agency to look across silos, objectively gauge which risks are directly aligned to achieving strategic objectives, and determine which risks have the greatest probability of impacting the mission. Risks that are determined to be significant are prioritized, vetted and escalated appropriately to agency leadership, where they can be regularly monitored, analyzed and considered as part of the agency's internal management routines. Opportunities and mitigation efforts are then incorporated into the agency's performance plan, an evolving document that is updated annually. With a shorter time horizon (two-year) than the strategic plan, the agency's performance plans are often more operationally and programmatically focused. Aligning strategy and performance to develop appropriate risk responses

through the planning process is critical to mitigating the influence of risks on achieving agency goals and objectives.

**Figure 2: ERM Linkages to Strategy and Performance**



Agencies should consider as a best practice coordinating the analysis of top risks with the strategic review. This integration of complementary processes can support the identification, assessment and prioritization of probable risks that may impact program delivery or outcomes and are likely to impact the success of a given strategic objective. One approach is to integrate ERM into an existing management process that can help agencies determine its strategic risks while mutually reinforcing the comprehensiveness of the organizational analyses required by each process.

The agency's strategic objective review process is an optimal time to coordinate an enterprise analysis of risk and make informed decisions. This allows the agency to reflect the compiled results of the analyses in proposals contained in the agency's budget submission, annual planning, and priority-setting. This includes identifying risks arising from mission and mission-support operations, providing a thoughtful analysis of the risks an agency faces towards achieving its strategic objectives, and developing responses that may be used to inform decision-making through existing management processes.

As part of the strategic objective review process, agencies can include as part of the Summary of Findings those risks considered by their agency leadership to be the top risks from their risk profile. Discussing these risks during the OMB Strategic Review meeting can be an opportunity to increase OMB's and the agency's shared understanding of the agency's needs and strategies. The identification of risks and risk management strategies around them may be used to inform changes to agency implementation strategies and future strategic and performance planning efforts. Agencies will need to coordinate the timing of the update to their agency risk profile to effectively inform the analyses and

assessment of strategic objectives being generated in the agency's Summary of Findings and for discussion with OMB.

Consistent with OMB Circular A-11, Part 6, agency Chief Operating Officers (often, the Deputy Secretary or Deputy Administrator) should, with the agency's Performance Improvement Officer, lead at least quarterly data-driven reviews to assess progress toward meeting the organization's priorities, including Agency Priority Goals. In some agencies, these are referred to as Quarterly Performance Reviews. These meetings are designed to review progress on the top priorities for the agency with agency leaders. Some agencies base the meetings on Agency Priority Goals while others conduct meetings with some or all of their bureaus and components. It is a good practice to incorporate in these meetings a discussion of risks to achieving those priorities as well as opportunities of pursuing risk to meet a stretch goal or objective. This helps focus leaders on the top risks to their priorities on a quarterly basis. These meetings can also be used to discuss crosscutting risks or challenges that may affect the achievement of objectives as discovered during the strategic objective review process. By incorporating risk in the quarterly performance reviews, agencies are better positioned to know more quickly how risk is affecting progress on priorities and adapt to changes in the operational environment in order to manage possible changes to strategies. Having regular discussions of risk, integrated with performance, helps evolve the organizational culture, build transparency, and inculcate risk terminology into strategic discussions.

### **Integration with Budgeting**

Aligning budgeting decisions and ERM assessments helps the agency understand possible risks and the funding available to mitigate those risks. When well executed, ERM improves agency capacity to prioritize efforts, optimize resources, and assess changes in the environment. ERM can help agency leaders make risk-aware decisions that impact prioritization, performance, and resource allocation. ERM offices should share the enterprise risk profile with the team developing the budget, so they understand the agency's top risks and the responses being proposed to address those risks, some of which may have resourcing implications. In partnership with the budget teams, some agencies include language on the consideration of risk into budget guidance.

---

### **Sample Risk Language for Budget Guidance**

#### ***Identifying Risks and Opportunities for Improvement***

Incorporating risk-based decision making into strategic planning, organizational performance management, and budget processes allows business units (BUs) to better allocate scarce resources to address the highest priority risks, enhance performance, drive efficiencies, and promote cost savings. BUs should consider risk factors from across their programs and use them as important inputs to these processes. In budget submissions, BUs should identify major risks to their mission and to the strategic objectives they support, then articulate existing risk response strategies and additional resources necessary to address these risks. Transparency, business practices, reporting, and governance help define the overall risk culture.

---

Clear, data-rich information on an agency's significant risks can help agency leadership make better risk-based decisions for internal budget allocation, especially when choosing where to pursue risks to add value, determine whether to seek additional funds, weigh funding trade-offs, and better justify to OMB

budget examiners why specific funds are needed. In addition, ERM can demonstrate inter-relationships between financial and programmatic risks to inform these decisions. Articulating or cross-walking ERM risks to agency funding requests builds the business case for funding decisions and integrates the budget process with the agency's ERM program.

**Table 1. Key questions for senior leadership conversations about risk, strategy, and budget**

Strategic Context	Resources Needed	Impact and Timing
<ul style="list-style-type: none"> <li>• What are the agency's top risks?</li> <li>• What is the time horizon to address the risks (e.g., short-term: 1-2 years; mid-term: 2-4 years; long-term: greater than 4 years)?</li> <li>• Do the top risks address all of the risks in the agency's programs and operations?</li> <li>• Is the agency already responding to these risks?</li> <li>• What actions is the agency taking to mitigate, avoid, accept, transfer, or pursue this risk? Do you agree with the response?</li> </ul>	<ul style="list-style-type: none"> <li>• Are there non-financial options, such as policy changes or process enhancements that would have the same effect?</li> <li>• If non-financial options are limited, how much will it cost the agency to address this risk?</li> <li>• Can the risk be addressed with current funding levels?</li> <li>• Does the agency have a business case to account for requirements and gaps?</li> <li>• Who is accountable?</li> <li>• Is it a one-time expenditure or recurring? For how long? When will it start?</li> <li>• Can resources be re-allocated to address the risk? If so, from which areas?</li> </ul>	<ul style="list-style-type: none"> <li>• What agency actions are important to take this year? Next year? Future years?</li> <li>• Is there a foreseeable return on investment or improvement in program performance or agency operations?</li> <li>• How did the analysis generated by the agency's risk profile inform the budget?</li> <li>• Are the agency's budget line items aligned with the agency's analysis of risks from the strategic review summary of findings and the risk profile?</li> </ul>

While an agency's budget will never be solely based on a risk-based decision, it is a good practice to incorporate a discussion of what risks an office/program is trying to manage by requesting additional funds and the tradeoffs involved in those decisions.

### **Evidence-building Efforts: Evaluation Officer and Learning Agenda<sup>9</sup>**

The Evaluation Officer plays a leading role in overseeing the agency's evaluation activities and capacity

---

<sup>9</sup> The “Foundations for Evidence-Based Policymaking Act of 2018” required CFO Act agencies to create the positions of Evaluation Officer and Chief Data Officer and required agencies to create multi-year learning agendas.

assessments, learning agenda (or evidence-building plan), and information reported to OMB on evidence. The Evaluation Officer also collaborates with, helps shape, and makes contributions to other evidence-building functions within the agency.

One of the Evaluation Officer's primary deliverables is a multiyear agency Learning Agenda. A Learning Agenda is a systematic plan for identifying and addressing policy questions relevant to the programs, policies, and regulations of the agency. The Learning Agenda, a stand-alone part of an agency's Strategic Plan, should align to the Strategic Plan and address priority questions across the entire agency. Developing the Learning Agenda offers a systemic way to identify the data agencies intend to collect, use, or acquire as well as the methods and analytical approaches to facilitate the use of evidence in policymaking. Learning Agendas allow agencies to more strategically plan their evidence-building activities, including how to prioritize limited resources and how to address potential information gaps that may inhibit the agency's effective management of risks identified through their ERM processes. The Learning Agenda should consist of "priority questions" that are meaningful and specific to the agency, including short- and long-term questions, as well as operational and mission-strategic questions. The intent is that answering the question could help drive progress toward achieving the agency's mission and strategic goals and objectives. ERM officials should work closely with their agency Evaluation Officer to develop priority questions to ensure an understanding of enterprise risks is built into agency evaluations and policy analyses.

### **Integration with Internal Controls**

Aligning internal control with ERM helps harness internal controls capabilities to create a more effective risk response. OMB A-123 requires that internal control activities be integrated under a larger ERM program; accordingly, internal control should be an integral part of risk management and ERM. ERM and internal control should be components of an agency's overall governance framework. 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 the organization's risks and opportunities and integrates that full spectrum into a portfolio view. This encompasses all areas of organizational exposure to risk, as well as internal controls that 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 the 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.

---

## ERM Pitfall

### ***Focusing too much on internal controls***

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

---

Leaders should understand how their offices align with the risk management structure and how it intersects 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 an RMC, the concept should be communicated 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.

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 2 highlights how traditional risk management activities complement ERM.

**Table 2: Comparison Between Traditional Risk Management and ERM**

Traditional Risk Management		ERM
	Risk Management (Project or Program)	Internal Controls
<b>Definition</b>	Coordinated activity within a component to proactively identify, assess, and manage risks to a specific project, program, or function in an organization. <sup>10</sup>	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. <sup>11</sup>
<b>Examples in Federal Guidance</b>	<ul style="list-style-type: none"><li>• OMB A-133 <i>Audits of States, Local Governments and Non-Profit Organizations</i></li></ul>	<ul style="list-style-type: none"><li>• <i>Standards for Internal Control in the Federal Government</i> (GAO Green Book)</li></ul>

<sup>10</sup> *Risk management – Guidelines*, International Organization for Standardization (ISO) 31000:2018.

<sup>11</sup> *Standards for Internal Control in the Federal Government* (United States Government Accountability Office (GAO) Green Book).

Traditional Risk Management		ERM	
	Risk Management (Project or Program)	Internal Controls	
	<ul style="list-style-type: none"> <li><i>Risk Management Requirements for the Federal Acquisition Certification for Program and Project Managers (FAC-P/PM)</i></li> </ul>	<ul style="list-style-type: none"> <li>Federal Managers' Financial Integrity Act of 1982 (FMFIA)</li> <li>OMB A-123 <i>Management's Responsibility for Internal Control</i></li> <li>Chief Financial Officers (CFO) Act of 1990</li> <li>Federal Financial Management Improvement Act of 1996 (FFMIA)</li> </ul>	<ul style="list-style-type: none"> <li><i>Enterprise Risk Management (2016)</i></li> <li>OMB A-123, Appendix A <i>Management of Reporting and Data Integrity Risk</i></li> <li>OMB A-11 (Section 260) <i>Preparation, Submission, and Execution of the Budget</i></li> </ul>
<b>Additional References</b>	<ul style="list-style-type: none"> <li><i>Risk management – Guidelines (ISO 31000:2018)</i></li> <li><i>Risk management- Risk assessment techniques (IEC 31010:2019)</i></li> </ul>	<ul style="list-style-type: none"> <li><i>Internal Control – Integrated Framework (COSO 2013)</i></li> <li>GAO Internal Control Management and Evaluation Tool</li> </ul>	<ul style="list-style-type: none"> <li><i>Enterprise Risk Management – Integrating with Strategy and Performance (COSO 2017)</i></li> <li><i>Management of Risk - Principles and Concepts, “Orange Book” (Her Majesty’s (HM) Treasury (United Kingdom))</i></li> </ul>
<b>Focus</b>	Selected risk areas and processes focused on effective program/project implementation or fraud, waste, 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.
<b>Emphasis and Application</b>	Compliance with planned scope, time, and cost, as well as identifying and organizing risks for any particular program.	Conforming to external reporting requirements (e.g., audit reports, identified material weaknesses). Focused on 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 audit guidance.

		Traditional Risk Management	ERM
	Risk Management (Project or Program)	Internal Controls	
Key Attributes	<ul style="list-style-type: none"> <li>Risks are traditionally based on program or project operational execution, with risk tradeoffs made across cost, schedule, and performance.</li> <li>Focus on risks is more forward looking than with internal controls but does not extend beyond scope of program or project.</li> <li>Some risk integration can occur but may not extend past the program or project level.</li> <li>Risk appetite and tolerance is usually not explicitly addressed.</li> <li>Requires domain and technical program or product expertise, in lieu of functional experience.</li> <li>Risks primarily viewed in a negative construct.</li> </ul>	<ul style="list-style-type: none"> <li>Primarily addresses traditional financial, compliance, transactional, and operational risks, with a focus on risk reduction through the application of discrete controls.</li> <li>Risk assessments traditionally review past performance and activities and are generally not forward looking.</li> <li>Risks are identified and managed on a siloed, non-integrated basis (e.g., financial reporting, human resources, physical security).</li> <li>Risk appetite and tolerance is usually not explicitly addressed.</li> <li>Requires specialized, functional skillsets (e.g., financial accounting, IT security).</li> </ul>	<ul style="list-style-type: none"> <li>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.</li> <li>Provides the potential for a fully integrated, prioritized, and forward-looking view of risk to drive strategy and business decisions.</li> <li>Allows for more risk management options through enterprise-level tradeoffs, versus a primary focus on reducing risk through controls.</li> <li>Risks can be viewed as threats and opportunities (positive risks).</li> <li>Explicitly addresses risk appetite and tolerance.</li> <li>Requires more general and interdisciplinary skillsets, beyond functional and domain knowledge.</li> </ul>

## **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 risk response 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 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 silos.
- Promoting accountability and integrity of the agency's work.
- 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.
- Be responsive to the evolving risk profile of the agency.

### **B. 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, programmatic, 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 prevent the categorization of risk from becoming 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 generally includes risk awareness, transparency, and the agency's attitude toward risk and how it is managed. Risk culture is a key indicator of how widely an agency's risk management policies and practices have been adopted, and reflective of basic underlying principles in approaching risk. 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 a particular standard or framework (e.g., *COSO Enterprise Risk Management—Integrating Strategy and Performance, June 2017*, (COSO 2017) or ISO 31000:2018), 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 the 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 to agency activities. It does not eliminate risk. While agencies cannot respond to all risks related to achieving goals and objectives, 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 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 travel 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 inherent in carrying out an organization’s objectives. Agencies should evaluate, prioritize, and manage risks to an acceptable level. It is important to have clearly expressed and well communicated risk appetite statements establishing thresholds for acceptable risk in the pursuit of objectives. 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.
- 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. 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 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 different models and approaches where possible.

9. **Planning Fosters a Culture of Resilience:** Risk management needs to be forward-looking, while also considering lessons learned 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 shortcomings 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 racial, ethnic, religious, gender, disability, generational, geographic affiliation, educational, occupational, and other factors.

## E. Maturity of Enterprise Risk Management 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 within 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 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. A more mature risk organization will help create a culture that embodies the principles 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 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 D](#).

---

### 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.

---

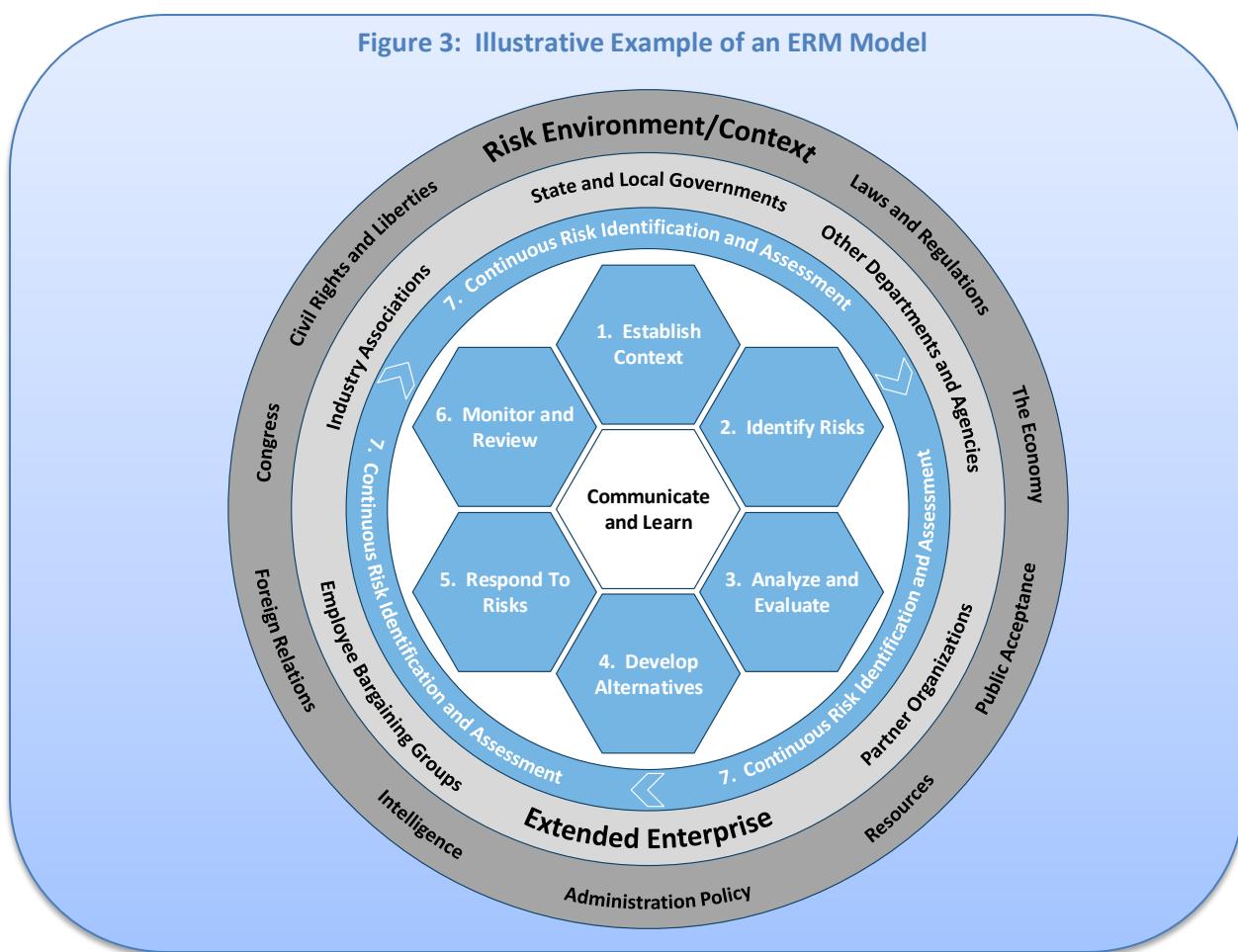
### III. Enterprise Risk Management Model

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's (COSO) *Enterprise Risk Management: Integrating with Strategy and Performance* (June 2017); 2) ISO 31000:2018; and 3) The United Kingdom's *Orange Book: Management of Risk – Principles and Concepts* (July 2019). 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 3 below. COSO's ERM 2017 highlights the value and role of integrating performance across an ERM framework, notably in risk identification, assessment, and responses (COSO Principles 10-14).

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 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.

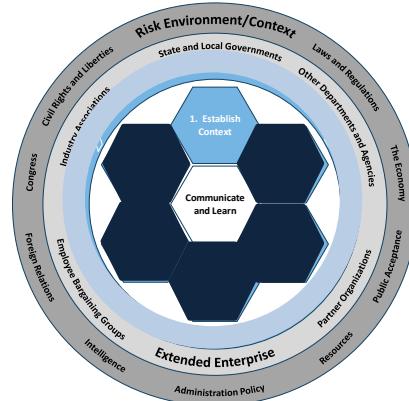
Figure 3: Illustrative Example of an ERM Model



## Step 1: Establish Context

Every agency functions within an environment that both influences the risks faced and provides the context in 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 mission and 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.

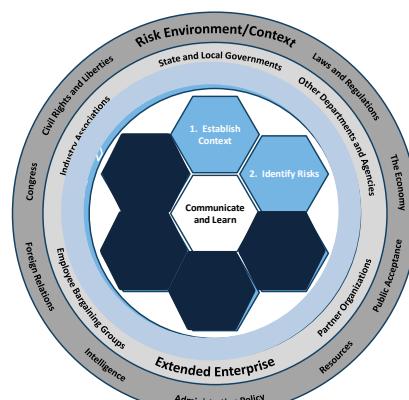


The first step in establishing the context is to determine the requirements and constraints that will influence the decision-making process, as well as key assumptions. This involves taking into consideration policy concerns, mission needs, stakeholder interests and priorities, agency culture, and the acceptable level for each risk, both for the agency in its entirety and for the specific program. Program managers should consider the control environment, delineating the safeguards in place to ensure compliance with applicable laws, regulations, and policies. Finally, agencies should consider how relevant stakeholders -- from partner organizations, other departments and agencies, other levels of government, industry associations, employee bargaining groups, Congress, the Judicial Branch, to 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](#).

## Step 2: Identify Risks

Agencies should use a structured and systematic approach to recognize potential risks and strive to address all key risks significant to the achievement of organizational objectives. As the ERM process becomes more formal, agencies may want to develop a risk register in which major risks are listed and their management plans are 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.



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](#).

---

## Tips for Documenting Risks

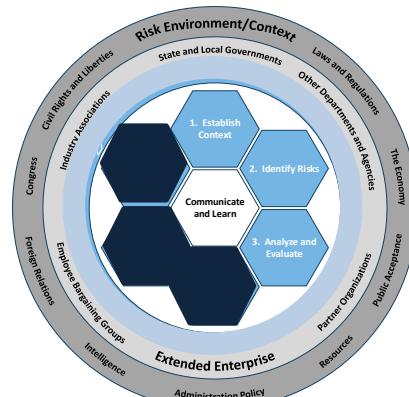
1. **Develop meaningful risk categories:** When defining or categorizing risks, agencies should consider categorization in ways that are most helpful and relevant to agency mission. Agencies should recognize that any single risk may be associated with more than one risk category and not limit risk categories to silos.
  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, 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.
- 

### Step 3: 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.

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](#).

#### Step 4: Develop Alternatives

Guided by risk appetite, agencies should (1) systematically identify and assess a range of response options or strategies to accept, avoid, pursue, reduce, transfer, or share major risks; (2) 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; (3) consider non-financial costs in terms of the reputational or political capital at stake; and (4) evaluate control options to respond to risk which may be preventative, corrective, directive, or detective in design.

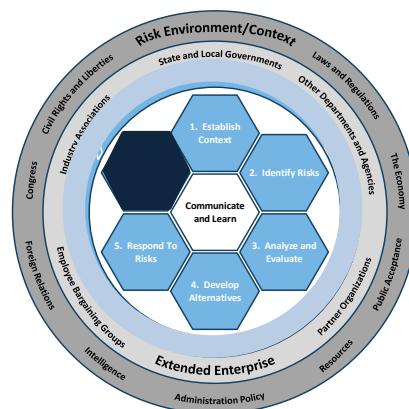
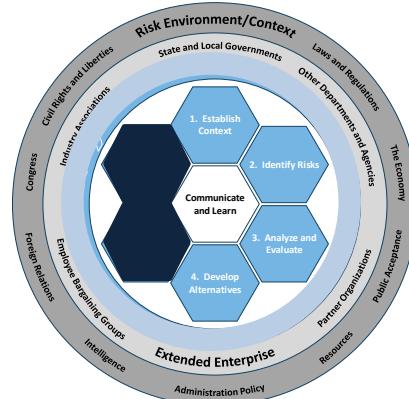
#### Step 5: Respond to Risks

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 its approach to managing particular risks if implementation fails to bring the risk within the organization's risk appetite.

#### Step 6: Monitor and Review

Agencies should regularly review, monitor, and update (as necessary) risk information in the enterprise-level risk profile to identify any changes and determine whether risk responses and risk response strategies are effectively mitigating risk. 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. 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 and RMC, for discussion.

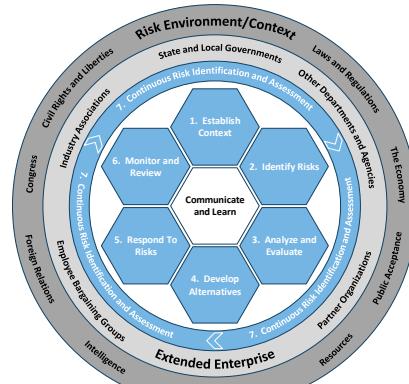
It is expected that this step will result in a risk register, dashboard, or other report to communicate the status of risk response activities. This includes whether an action has been started, completed, or delayed, and whether the action taken had the desired effect on the risk. It can also show what 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.

### Step 7: 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's culture it is 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 for ERM 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 agencies to 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.

## IV. Developing an Enterprise Risk Management 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 a 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 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. Culture and 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 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 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 establish an RMC, chaired by the COO or a senior official with responsibility for the enterprise. In Cabinet level agencies, this is the Deputy Secretary. An option is to leverage an existing governance forum to perform the function of an RMC. The RMC should meet regularly (e.g., monthly) to consider a range of major risks. It is essential 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. In driving a risk management culture throughout the organization, it is recommended that other governance and oversight forums (such as functional, domain, or lines of business) routinely consider risk and risk management in their deliberative processes.

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 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](#).

## B. Organizational Design, Alignment, Leadership and Staffing

---

### 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 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.

---

In developing an ERM capability in agencies, the organization's structure and culture must consider specific roles and responsibilities to guide ERM practitioners for ERM to be successfully embedded within the agency. There is no single, optimal alignment of function, organizational design, or staffing model for an ERM capability in an agency. A number of factors must be considered in the organizational design, functions, and staffing of an ERM capability, to include:

- Organization size, scope, and complexity
  - What is your organization's mission or range of projects, programs, and activities and how are you currently addressing uncertainty, challenges, and issues?
  - How does your agency define "enterprise?" As CFO Act agency, non-CFO Act agency, quasi-governmental? Is the "enterprise" a bureau or component that is either subordinate or aligned to a Cabinet-level agency?
- Organizational Level
  - Are you managing ERM for an organization (agency, subordinate bureau, or component), a single function (or portfolio), or multiple functions (portfolios) within an organization?
- Reporting & Governance
  - Will the ERM lead role report directly to the head of the agency or deputy head of the agency?
  - Aligned under Chief Financial Officer, Performance Management, or other C-suite function (e.g., strategic planning & internal controls function, and/or program analysis & evaluation).
  - Would the development of a CRO position benefit the organization by bringing together disparate functions with varying views and responsibilities?

- Would a Senior Risk Management Council advance ERM for your organization? What are the roles and responsibilities of a Senior Risk Management Council, and should it be a stand-alone forum or integral to a capstone management forum?
- Are there current governance groups where risk discussions could be embedded to leverage and advance ERM across the agency?

### **Functions**

At the CFO Act agency-level, the ERM program office may be more involved in setting policy, providing oversight, and coordinating activities, such as training across component bureaus or subordinate agencies. At the component/bureau level or below, the focus may be more on risk ownership or data collection, analysis, and tracking/reporting trends to senior leadership within the component/bureau or to headquarters. Typical functions of an ERM capability may include:

- Policy development
- Oversight of enterprise risk management and integration of risk management into operations
- Data/information collection, organization, and analysis
- Forecasting
- Tracking and reporting
- Environmental/mission/business function trend analysis
- Individual and collective training

### **Leadership/Staffing**

Depending on a number of factors (to include those listed above, leadership of the organization's ERM capability (i.e., Chief Risk Officer) may be a primary or collateral duty. Questions to ask and when creating roles, qualities of ERM practitioners, and example position descriptions can be found in [Appendix B, Part 2.](#)

## **VI. The Risk Appetite Statement**

### **A. What is Risk Appetite and Risk Tolerance?**

#### **Risk Appetite**

Risk appetite is the amount and type of risk an agency is willing to accept on a broad level in pursuit of its strategic or program objectives, given consideration of costs and benefits. An appropriate risk appetite should be established and communicated by the agency's most senior level leaders to serve as the guidepost to drive risk-informed decision making on developing strategy and objectives, allocating resources, and managing performance outcomes. Without defining risk appetite, an agency may take more or less risk than may be appropriate to achieve its objectives. However, risk appetite is useful only if it can be cascaded down, interpreted, and utilized by employees at all levels within the agency to determine tradeoffs and take actions consistent with the agency's intent.

Clearly expressed and well-communicated risk appetite statements can provide guidance on the amount of risk that is acceptable in the pursuit of objectives or goals and can help policymakers make informed decisions. Defining risk appetite can also enable agency management at various levels to make risk-

informed decisions on allocation of resources, management controls, and potential impacts to other parts of the agency. It can reduce surprises and unexpected losses. A practical approach is recommended. Discussing qualitative aspects and the overall appetite for various types of risks is more important than trying to apply a quantitative formula or mathematical precision regarding such risks.

### **Risk Tolerance**

To implement its risk appetite, an agency needs to clarify how the overall risk appetite should be translated at operational levels to achieve desired outcomes. Risk tolerance is the acceptable level of variance in performance relative to achievement of established objectives. In other words, risk tolerance translates risk appetite into meaningful terms at the operational level. It is usually defined at the objective, operational unit, program, business process, or component level. Measuring and then tracking the alignment of the agency using existing metrics is an effective way to ensure alignment with the agency's desired risk appetite for that function, product or service, goal, or objective. In setting risk tolerance levels, the agency should align the tolerance with the associated risk appetite and determine if the performance of an objective is within the acceptable risk range, both qualitatively and quantitatively.

### **Why Develop a Risk Appetite Philosophy?**

While risk appetite is a relatively new concept for certain federal agencies, risk appetite principles have been in existence in the private sector for decades. In a complex world where the federal government is tasked with responding to events and actions that are happening simultaneously and rapidly, agencies need to use a clear and cohesive approach to manage multi-level activities as efficiently as possible.

Developing and using risk appetite principles to manage strategic objectives and operations can help agencies directly align their day-to-day activities with senior leaders' expectations of getting results for their agency and provide the agency with assurance that employee efforts are aligned with leadership's direction. Assessing risk appetite is a valuable endeavor for agencies to ensure risks taken within the business are within acceptable limits and that strategic opportunities are not missed due to assumed risk aversion.

### **Context is Critical**

Context is critical to any discussion on risk appetite. For example, an agency may be willing to accept very little risk with regard to the safety and health of its employees and visitors but more willing to accept risk in areas such as first-of-its kind technology or innovation. Active considerations of tradeoffs are necessary and senior management needs to define where tradeoffs are or are not acceptable.

Agencies can determine the most effective manner to assess and update risk appetite. While broad statements on risk acceptance can be made, it is usually more helpful to define risk appetite in various contexts and informed by goals or missions of the agency or program. A single risk appetite statement can include these different aspects, or separate risk appetite statements can be defined for each aspect.

For example, agencies may want to define risk appetite by:

- Strategic goals or objectives
- Existing Risk Profiles
- Existing Risk Categories or Risk Types
- Key programs and mission support functions

- Core products and services
- Core values of the agency

This concept is discussed further in Section C, “Methods for Establishing a Risk Appetite Statement.”

## C. Methods for Assessing and Updating Risk Appetite

An agency should assess what its risk appetite is today, and whether senior leadership is comfortable with that risk appetite level. If the agency’s senior leadership is not comfortable, then it should communicate what an appropriate risk appetite level should be, ways to achieve it, and timeframes within which to achieve it. This will help an agency focus its efforts on those areas where the greatest misalignment may be occurring. To support an initial assessment of risk appetite, an agency can use its current risk profile as a basis for discussion with senior leaders on acceptable levels of risk. In the absence of an agency level risk profile, a concerted effort should be devoted to assessing the agency’s current risk exposure. This will help senior leaders to project how much risk they are willing to take in a foreseeable future. The risk appetite should be reassessed when leadership changes or when the goals and objectives of the agency change to keep it relevant.

Several tools, techniques, and methods available to agencies to assess their agency’s risk appetite are discussed below.

### Utilize a Risk Scale

A tool to assist organizations in determining risk appetite is to establish a risk scale. This helps to articulate how much risk an agency is willing to take in order to achieve its objectives, and can be used to assess where the organization is today to inform areas where gaps exist and alignment is necessary. Figures 1 and 2 below provide samples of risk appetite scales that offer descriptions of risk appetite levels according to various approaches or objectives.

**Table 3: Sample Risk Appetite Scale by Approach**

Risk Appetite Approach	Very High Risk Appetite	High Risk Appetite	Moderate Risk Appetite	Low Risk Appetite	Very Low Risk Appetite
Potential Loss vs. Opportunity Loss	Agency is willing to take aggressive risks to achieve strategic objective	Agency is willing to take greater than normal risks	Agency weighs the risks of potential loss against the lost opportunity gained from the risk	Agency is willing to accept less efficiency and effectiveness to avoid taking risk	Agency takes caution and often accepts as little risk as possible, regardless of opportunity loss
	Agency is willing to accept a negative impact to achieve a goal	Agency is willing to accept some negative impact to achieve a goal	Agency considers the negative impact and achievement of a goal of equal importance	Agency is only willing to accept a small negative impact to achieve a goal	Agency is not willing to accept a negative impact to achieve a goal
	Minimal controls to address risks	Agency develops controls when a strong case can be made for cost effectiveness	Agency controls when a case can be made for cost effectiveness	Agency develops controls even if their cost outweighs potential negative impact	Agency develops controls regardless of cost to minimize potential risk
	Risk is accepted as much as the Department/ Congress permits	Preference to accept some risk and damage it through limited controls	No preference to reduce or accept risk	Preference to reduce risk as much as possible through controls	Preference to avoid risk unless it can be easily managed

**Table 4. Sample Risk Appetite Scale by Objective**

Rating	Risk Taking Philosophy	Tolerance for Uncertainty – How willing are you to accept uncertain outcomes, whether positive or negative?	Choice – When faced with multiple options, how willing are you to select an option that puts the objective at risk?	Trade-off – How willing are you to trade off this objective against achievement of other objectives?
5 - Open	Will take justified risks	Fully anticipated	Will choose option with highest return; accept possibility of failure	Willing
4 - Flexible	Will take strongly justified risks	Expect some	Will choose to put at risk, but will manage the impact	Willing under certain conditions
3 - Cautious	Preference for safe delivery	Limited	Will accept if limited and heavily outweighed by benefits	Prefer to avoid
2 - Minimalist	Intentionally conservative	Low	Will accept only if essential, and limited possibility/extent of failure	With extreme reluctance
1 - Averse	Risk avoidance is a core objective	Extremely low	Will select the lowest risk option, always	Never

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

Using a common scale in interviews and/or surveys across the agency can help ensure that employees and management are using the same terms to define and communicate risk appetite and can clearly articulate how much risk management is willing to take to achieve a specific goal.

### **Hold Brainstorming Sessions with Key Stakeholders**

Risk appetite levels should be developed by merging the ideas of several tiers of management, with top leadership approval and influence on the final risk appetite statement. The most senior members of an agency should be involved in setting overall risk appetite levels in conjunction with goals and objectives and keeping in mind budgetary constraints. Program owners and business line managers should also be consulted about their top risks and how they monitor them. These facilitated discussions will allow for risk appetite to be developed with business lines in mind so risks can be consistently managed in a language that is familiar to all within the agency. Among both senior members and managers, risk appetite should be considered within the context of established laws, regulations, standards, and rules.

### **Conduct a Survey**

Another method of gaining a top-down and bottom-up assessment of your agency's risk appetite levels is to send select stakeholders a tailored questionnaire or survey on risk appetite. Such a questionnaire can gauge how much risk senior members and project and business line managers are willing to take to achieve certain goals or objectives. In conducting the survey, a common risk appetite rating scale should be used to summarize and compare the inputs, as discussed above. The data can then be used to identify potential gaps in risk tolerance between different business lines and/or different levels of seniority. It can also help to gauge potential blind spots in the agency's risk culture. These are areas in which improved communication of leadership's expectations can help business lines take the right amount of risk and effectively communicate potential warning signs of increased exposure to risks that agency has deemed unacceptable.

### **Conduct Structured Interviews**

Structured interviews can help to assess an agency's risk appetite. After identifying the proper stakeholders, interviewers can ask a set of prepared questions to encourage interviewees to present their perspective on strategic goals and objectives, as well as their business line's goals and objectives. These answers can then be aggregated to better identify common areas where the agency is willing to take more or less risk. Similar to the survey approach, a common risk appetite rating scale should enable a roll-up and analysis of interview results to inform recommendations to management.

### **Hold Periodic Reviews of the Risk Appetite Statement**

Once a risk appetite statement is established, the frequency by which senior management reviews the statement should be discussed during brainstorming sessions or structured interviews with key stakeholders. A common trigger to revisit risk appetite is when an agency's top leadership changes. A new agency head can bring in a very different perspective on acceptable risk than the predecessor. When leadership is in place, the risk appetite review could be an annual exercise to provide timely guidance and immediate direction to managers on budget formulation, performance review and reporting, and annual risk and control assessments; or, the risk appetite statement could be defined in a way that stands the test of time in that it is linked to core mission or values of the agency that are not subject to annual change. While application of risk appetite may vary from agency to agency, it is recommended to consider the period of applicability for the risk appetite statement early in the process

to avoid unnecessary misaligned expectations.

## D. Methods for Establishing a Risk Appetite Statement

An agency typically establishes a risk appetite statement to communicate its intent with regard to risk acceptance and to establish risk tolerance levels across the agency. Risk appetite statements can be developed at the agency level, at functional levels, in accordance with strategic objectives, at program level, or in other targeted categories that make sense to the agency. It should be noted that risk appetite statements are not required under OMB A-123 or OMB A-11. However, these can be a useful tool for top-down communication when established.

While we focus on two examples below, using an agency's strategic objectives or mapping to a risk category or type, there are multiple methods for developing risk appetite within an agency. Other categories of consideration include mapping risk appetite to the agency's core products, services, or values. These critical agency outputs typically draw a clear, red line for the agency to inform trade-off discussions – some aspects cannot be placed at risk at any costs, whereas others may be more flexible. Outlining these parameters can help identify where the “trade space” exists, and where it does not.

The maturity of the ERM Program, the agency's risk culture, and the nature of the agency's mission, vision, and goals will all contribute to how an agency will draft and communicate a risk appetite statement. No matter which method is used, it should be clear and concise, and employees should be able to use it to make risk intelligent decisions. The following are various examples of how to approach developing a risk appetite statement.

### Focus on the Agency's Strategic Objectives

Risk appetite should be informed by the public policy purpose of the program, the agency's budget, 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.

By understanding an agency's strategic objectives, leadership's direction and focus, and funding streams, it is possible to establish a risk appetite statement around how much risk the agency is willing to take to achieve those objectives, relative to its other basic objectives (e.g., health and safety of employees, protection of assets and infrastructure, etc.). Using strategic plans, performance reports, and capability models to link an agency's risk appetite to concrete objectives will help to build consistency by using language that is already familiar within the agency.

### Map Risk Appetite to Risk Category or Risk Type

A risk appetite statement should identify what level of risk the agency is willing to accept in pursuing its mission, goals, and objectives. This level of specification enables clear communication on what risk that agency is willing to accept or not accept. Often, this specificity can be provided by mapping risk appetite

to existing Risk Categories or Risk Types as defined by the agency. For example, if an agency's long-term objective is to end the need for providing foreign assistance overseas, the agency may want to take more risks to capitalize local ownership and resources in host countries. Therefore, having a category or type called "Programmatic Risk" on the agency's risk appetite statement sets a clear tone from the top and guides all levels of management when designing and implementing development programs. While categorizing risks provides a broad parameter for certain type of risks an agency is willing to take or not, further delineating different level of risk appetites within a category or type can promote risk ownership, stakeholder engagement and lead to developing risk tolerances.

In another example, if an agency's mission is to provide services solely for its customers, the agency may choose to be more conservative in taking operational risks that would significantly interrupt its customer service versus agency's internal operations. Because different offices within the agency are responsible for internal and external operations, it should be easier to identify risk owners and key stakeholders to manage risks to acceptable levels.

## **E. 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 and the policy goals they are trying to achieve. In doing so, agencies may adopt rating scales, such as a scale ranging from 1-5, and set relative differences across the levels. Agencies should consider the relationship and consistency of the scale they use to assess enterprise risks when developing the scale for risk appetite statements. Agencies should also be able to communicate and articulate the level of risk they are willing to accept to meet or exceed the desired outcomes.

Writing a risk appetite statement is not just about writing a one-off, standalone statement to drive risk-based decision making. Its effectiveness is based on how it relates to existing agency components and how well it is understood throughout the agency. Therefore, it is imperative agency employees understand how risk appetite fits into the risk management framework. Risk appetite should (i) directly link to agency objectives, (ii) be worded clearly and specific enough so it can be communicated throughout the agency, effectively monitored, and adjusted over time; (iii) help with setting acceptable, measurable risk tolerances; (iv) facilitate the alignment of agency people, processes, and infrastructure in pursuit of agency objectives; and (v) facilitate the response to and monitoring of risks. Further, the risk appetite statement should evolve as the agency does. Senior leadership should review and update the risk appetite statement annually or at least during the revision of the agency's strategic plan to ensure the appropriate amount of risk is being taken to achieve new or changed goals.

When establishing risk tolerance, agencies should use existing metrics used to measure performance whenever possible. For example, an agency that accepts a certain failure rate, error rate, response time, or processing time has already set parameters for acceptable performance. These same parameters can be assigned a risk tolerance level and utilized as red flags to identify when the agency is straying outside of its established guideposts. These metrics can also be used to assess when the agency is too narrowly interpreting risk appetite or when it is straying outside of the desired limits. Other existing performance metrics may already be defined by the agency under the GPRA Modernization Act. These establish performance metrics that are tracked for reporting against agency strategic plans and can be a foundation for risk tolerance discussions. For example, operations and project teams may follow the course of long-standing business practices, but these practices may reflect an inherent risk aversion that is considered too narrow by the agency's leadership. When agencies explore how to expand the

guideposts, they need to translate what changes are needed at the operational level to reset the understanding of risk acceptance. This reflects top-down influence on the agency. In some cases, new metrics may need to be established to track alignment with the agency's risk appetite. When this occurs, agencies should ensure that the time invested in creating and tracking metrics outside of existing systems provides meaningful value and insight. Periodically assessing the alignment of the agency with risk appetite using the metrics defined at the operational level is good business practice.

## F. Examples of Risk Appetite being applied in an agency

Risk Appetite, once established, can be utilized in a variety of contexts. A well-defined risk appetite can assist staff at various levels to make risk-informed decisions with regard to the actions the agency will take in responding to risks in pursuit of its goals and objectives, allocation of resources, management controls, and potential consequences or impacts to other parts of the agency. The following examples show how risk appetite can be built into existing agency processes.

### Incorporating Risk Appetite within Enterprise Risk Management Program

The agency ERM function typically supports senior leadership in assessing risk appetite, establishing risk appetite statements, and facilitating dialogue with operational teams to translate a risk appetite statement into actionable terms. The ERM function establishes the value proposition with senior leaders of understanding and defining agency risk appetite. In addition, risk appetite can be a method of facilitating discussion on the agency's exposure to changing internal and external risks and its ability to adapt.

Federal agencies have various levels of ERM program maturity; however, the majority of agencies have developed an enterprise-level risk inventory, or agency "risk profile." Some agencies have developed risk response plans for those risks identified on their agency risk profiles. An approved risk appetite serves as a guidepost and helps agencies prioritize which risks to respond to first. Aligning overall agency risk appetite with specific risks from its risk profile drives risk-informed decision making on which risks should be considered for further action, which may require resource investments in the coming years.

Comparing risk appetite to the risk rating for top risks at the agency can inform leadership as to where gaps exist and where risk appetite may be misaligned with the level of risk at hand. For example, in the figure below, the agency has established a "Low" risk appetite for Information Technology. However, the related Information Security risk was rated as "High." This immediately identifies a gap where a risk response is necessary and should be prioritized.

**Table 5. Sample Mapping of Risk Appetite to Risk Ratings to Inform Risk Response**

Risk Appetite Statement		Risk Profile Information			Risk Response
Risk Category	Overall Risk Appetite	Risk	Risk Score Rating	Executive Owner	
Strategic	Moderate	External Stakeholder Engagement	12 Medium High	External Affairs Director	Accept
Operational	Low	Acquisition/Procurement	15 Medium High	Procurement Executive	Reduce
Information Technology	Low	Information Security	20 High	Chief Information Security Officer	Reduce
Legal	Low	Compliance	3 Medium Low	General Counsel	Accept
Program	Moderate	Fraud	20 High	Chief Operating Officer	Reduce

#### Incorporating Risk Appetite in Budget Formulation

When determining resource allocation, it can help to consider how a reduction in budget could negatively impact the agency's ability to accomplish its strategic goals and objectives. By listing those objectives and asking business lines if a budget reduction could impact those objectives and, if so, how, senior management can better allocate resources to different business lines depending on how much risk the agency is willing to take.

**Table 6. Appetite in Budget Decision-Making**

Agency Strategic Objectives	Will Budget Reduction Affect Objective?		Appetite for Risk
	Business Line 1	Business Line 2	
Objective A	Yes	Yes	Low
Objective B	Yes	No	Low
Objective C	No	No	Moderate
Objective D	No	Yes	High
Objective E	No	Yes	High

In the above example, the agency should carefully consider how much to reduce Business Line 1's budget as it could affect Objectives A and B, for which the agency has a low risk appetite. Similar consideration should be given to Business Line 2's budget, while considering that it could affect Objectives A, D and E – one of which the agency has a low risk appetite for and the other two a higher

risk appetite.

### **Incorporating Risk Appetite into Strategic Planning and Performance Reviews**

If risk appetite is how much risk an agency is willing to accept to achieve its goals and objectives, then it stands to reason that when establishing strategic goals and objectives, it is important to incorporate the agency's existing risk appetite and examine whether the risk appetite or the agency's goals should be modified. Oftentimes the desire for increased efficiency and effectiveness can come at the expense of increased exposure to risk in other areas. By incorporating a review and revision of the risk appetite statement at the same time strategic goals and objectives are being established, an agency can review how closely it wishes to engage in new goals and objectives as well as identify how much risk it is willing to take on to achieve such goals. Similarly, considering risk appetite when conducting strategic reviews presents an opportunity to check alignment of risk acceptance with the progress the agency may or may not be making in achieving its established goals and objectives. A change in course may be identified to ensure success by the timeframes pursued for a given objective.

As noted earlier, the arrival of new leadership typically triggers a reconsideration of risk appetite across many facets of the agency, but most immediately as related to the leader's strategic goals and objectives. Risk appetite that is tied more closely to operational metrics that are core to the agency's mission or existing risk categories are less likely to be influenced by frequent change at the top.

### **Incorporating Risk Appetite into Procurement**

When identifying capabilities to acquire, systems to upgrade, or architecture to build, it's important to consider the agency's appetite for risk. A simple set of questions can be established in the acquisition process to strengthen the business case to help senior management to determine whether to procure a particular capability (commodity and/or service) or to pursue an innovative acquisition practice. Sample questions below highlight how risk appetite can be incorporated.

Questions	Application to Risk Appetite
What risks could materialize if the initiative is not approved?	<ul style="list-style-type: none"><li>▪ What appetite does the agency have for these types of risks?</li></ul>
What risks could prevent successful implementation of this initiative?	<ul style="list-style-type: none"><li>▪ Are these risks within the agency's appetite for risk?</li><li>▪ What controls are in place to make sure these risks can be brought within the agency's appetite?</li></ul>
How would this initiative address or reduce risk within the agency?	<ul style="list-style-type: none"><li>▪ Will this initiative alleviate an existing risk that is outside the agency's risk appetite?</li></ul>
How can we better achieve the mission?	<ul style="list-style-type: none"><li>▪ What innovative acquisition practices could be pursued to achieve the mission while remaining compliant with laws and regulations?</li><li>▪ What are the risk/reward tradeoffs of pursuing these options?</li></ul>

# VII. Developing a Risk Profile

OMB A-123 requires each agency to develop a “risk profile.” OMB 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 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 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 have discretion in terms of the appropriate content and format for their risk profiles. However, OMB A-123 calls for agencies to include the following seven components:

1. Identification of Objectives
2. Identification of Risks
3. Inherent Risk Assessment
4. Current Risk Response
5. Residual Risk Assessment
6. Proposed Risk Response
7. Proposed Risk Response 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 OMB 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 1: Identification of Objectives**

Agencies should begin by identifying their objectives. There are four objective categories outlined in OMB’s A-123: strategic, operations, reporting, and compliance. These four categories align with the Strategy & Objective-Setting component of the *COSO 2017* guidance. 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, the relevancy of risk depends on the context of the organization’s objectives. OMB 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.

**Table 7: Objectives as outlined in OMB A-123 and their corresponding risk categories**

A-123 Objective	Corresponding Risk Category
<b>Strategic:</b> Relating to the strategic goals and objectives aligned with and supporting the agency's mission	<b>Strategic Risk:</b> 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.
<b>Operations:</b> Relating to the effective and efficient use of the agency's resources related to administrative and major program operations	<b>Operational Risk:</b> 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.
<b>Reporting:</b> Relating to the reliability of the agency's reporting	<b>Reporting Risk:</b> 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.
<b>Compliance:</b> Relating to the agency's compliance with applicable laws and regulations	<b>Compliance Risk:</b> 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 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 2: 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. COSO 2017 elevates and highlights the elements of performance when it comes to the principles of identification, assessment, prioritization, risk responses, and portfolio view with performance woven into the process.

Information captured for each risk should include the related strategic objective, if applicable, whether the risk is in fact a control deficiency or high-risk area previously identified, and any risk response plans, corrective action plans, or management 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.

---

### **Sources for Identifying Risks**

- **Agency Reports and Self-Assessments**
  - Anything raised during Strategic Objectives Annual Review, quarterly performance reviews, RMC, etc.
  - Project management risks documented in the agency's investment and

- project management processes.
- Previous year Federal Managers and Financial Integrity Act reports and OMB 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.
  - **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 any particular major risks cause an impact?

---

## 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? How can we support you in better managing them?

---

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.

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 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 multiple strategies need to be devised. Understanding all the possible risks will help an agency develop a thorough response strategy.

### **Step 3: 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.<sup>12</sup> 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 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 internal stakeholders. Root-cause analysis can help an agency link otherwise disparate occurrences and determine 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 A-123) are shown below:

**Table 8: Example of a Risk Impact Rating Scale**

Rating	Description
<b>High</b>	The impact could preclude or highly impair the organization’s ability to achieve one or more of its objectives or performance goals.
<b>Medium</b>	The impact could significantly affect the organization’s ability to achieve one or more of its objectives or performance goals.
<b>Low</b>	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.

---

<sup>12</sup> Some agencies may not rate the likelihood and impact of inherent risks because existing controls are already in place to mitigate many inherent risks and rating an inherent risk could require the agency to assign a rating that assumes the pre-existing controls are absent. Such an exercise may not produce the highest value to the organization. Thus, agencies may only rate the likelihood and impact of residual risks.

**Table 9: Example of a Risk Likelihood Rating Scale<sup>13</sup>**

Rating	Description
<b>High</b>	The risk is very likely or reasonably expected to occur.
<b>Medium</b>	The risk is more likely to occur than unlikely.
<b>Low</b>	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. The impact may also be affected by how quickly a risk could materialize, also known as 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 your priority risks will require actions. At this point it is recommended 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?

---

<sup>13</sup> Likelihood may be based on the risk occurring in a given period of time as determined by the agency.

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 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 in its entirety.

#### **Step 4: Current Risk Response**

Risk responses are the actions taken to manage or treat risks. Types of risk responses may include:

- **Accept:** 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.
- **Avoid:** Action is taken to stop the operational process, or the part of the operational process causing the risk.
- **Pursue:** Action is taken to increase risk in pursuit of opportunity (see COSO 2017 update).
- **Reduce:** Action is taken to reduce the likelihood or impact of the risk.
- **Share:** 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 OMB A-123 Internal Controls team to ensure these risk items are addressed and included in OMB A-123 testing.

---

#### **OMB 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. Risk response strategies help agencies identify actions and priorities to include in performance plans.

Key questions to consider during this step include: What actions will be taken to accept, avoid, pursue, transfer, reduce, or share our risks? Are these actions actually managing 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 5: 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 in 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 the 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 OMB 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 6: Proposed Risk Response**

Proposed risk responses are planned or suggested actions to further reduce residual risk. After agency senior leadership has completed its 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 manage 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 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 7: 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.

## **G. 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 OMB Circulars A-11 and A-123, agencies should include in their Strategic Objective Summary of Findings (which are submitted to OMB) key risk information from their risk profiles so that their overall assessment of strategic objectives, including risks, can be discussed as part of the Strategic Review meetings between the Agency and OMB.

## VIII. GAO/OIG Engagement

As stated in OMB 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 OIG, 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. Special Chapter: Integration of Agency Enterprise Risk Management with Information Security and Cybersecurity Risk Management

How a federal agency handles and protects its assets can directly impact its reputation, compliance, and effectiveness. Information security, cybersecurity, privacy, and related risks have been consistently cited by federal ERM program managers as top areas of risk. This chapter is intended to support the understanding of agency-level enterprise risk officers and ERM program managers of these more technical areas of risk and how to better integrate risk management efforts within these functional areas with agency ERM to improve decision-making.

### A. Foundations of Information Security and Cybersecurity

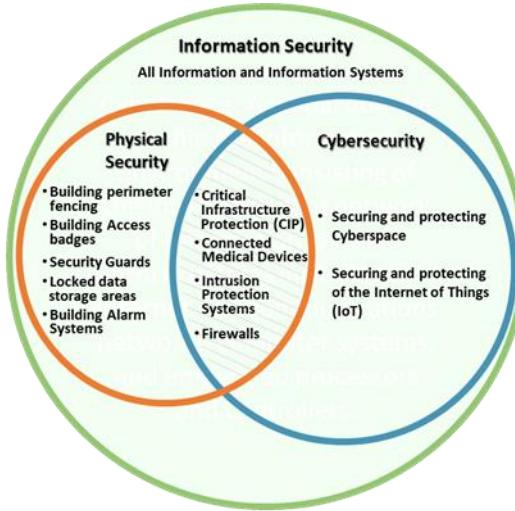
There is often a lack of clarity and awareness about the differences (see [Appendix J](#)) between “information security” and “cybersecurity.” These terms are frequently used synonymously to describe the security of information and systems; each plays a role in the security and protection of information and information systems from threats and data breaches. Figure 4 helps define these differences.<sup>14,15</sup>

---

<sup>14</sup> The intersection of physical security and cybersecurity addresses Critical Infrastructure Protection (CIP) such as the electric grid, financial systems, Supervisory Control & Data Acquisition (SCADA) systems and Industrial Control Systems (ICS). Cyberspace is a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

<sup>15</sup> Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102.

**Figure 4: Relationship Between Information Security, Cybersecurity & Physical Security**



**Information security** is the “protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.”<sup>16</sup> It includes protecting information in both digital and non-digital forms anywhere (physical or cyberspace). Physical controls must be implemented along with administrative controls (e.g. policies and procedures) and technical controls (e.g. intrusion detection systems, firewalls) to reduce risk to organizational information and systems.<sup>17</sup> This includes managing risks related to mobile devices, such as laptops, tablets, and smart phones, due to their use in locations outside the organization’s control.<sup>18</sup> [NIST Special Publication \(SP\) 800-53A](#) provides specific guidance on assessing controls in information security program plans, privacy program plans, system security plans, and privacy plans. Additionally, Executive Order [13556](#) established a government-wide Controlled Unclassified Information (CUI) program to standardize the way the executive branch handles unclassified information that requires protection. NIST [SP 800-171](#) provides recommended requirements for protecting the confidentiality of CUI.

**Cybersecurity** protects information technology systems against unauthorized use of electronic data. This may result in disruption of hardware, a tangible asset, or an intangible asset. Examples include disruption to organizational missions, privacy, reputation, public confidence, information, software, and intellectual property.<sup>19</sup> Adverse impact on tangible and intangible assets can potentially lead to harm to affected persons or society. A Cybersecurity Maturity Model Certification (CMMC) has been developed to provide a unifying standard for the implementation of cybersecurity across the Defense Industrial Base (DIB) and serves as a verification mechanism to ensure that DIB companies implement appropriate cybersecurity practices and processes to protect Federal Contract Information (FCI) and CUI within their

<sup>16</sup> [NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations](#), Dec 2018.

<sup>17</sup> [NIST SP 800-12 Rev. 1, An Introduction to Information Security](#), Jun 2017.

<sup>18</sup> [NIST SP 800-124, Guidelines for Managing the Security of Mobile Devices in the Enterprise](#), Jun 2013.

<sup>19</sup> [NIST SP 800-160 Vol. 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems](#), Section 2.3, Nov 2016, Updated Mar 2018.

unclassified networks.

**Physical security** protects people, data, equipment, systems, and facilities from physical loss or harm. It includes protection from natural disasters and criminal activities such as espionage, theft, and terrorism. Cyber-physical systems or the “Internet of Things” (IoT) have become an increasing area of risk due to the prolific use of “smart” devices with internet capabilities. Strong policies and controls related to cyber supply chain risk management will also strengthen physical security.<sup>20</sup> The organization must take proper measures to ensure that their IT and information security vendors are trustworthy and verified through effective procurement practices.

### **Foundations of Risk in Information Security**

An enterprise-wide information security risk management strategy allows organizations to effectively manage risk to assets and missions and to reduce the likelihood of breaches and data loss.<sup>21,22</sup> Information security risk management uses many of the principles of a traditional risk management process to frame risk, assess risk, respond to identified risks, and continuously monitor risks. NIST’s seven-step framework offers a specific approach and process to risk management that “integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle.” As a framework, it is flexible enough so that it can be applied to new and legacy systems, any type of system or technology, and across various organizational types, sizes, or sectors. The NIST seven-step framework consists of Prepare, Categorize, Select, Implement, Assess, Authorize, ad Monitor.

Organizations must clearly understand their mission and how each asset supports it.<sup>23</sup> In conducting risk management, the organization should document how it frames risk (i.e., how it establishes the context for risk-based decisions) through<sup>24</sup>:

- Assessment of threats, vulnerabilities, probabilities, potential impacts, or other attributes of an event.
- Constraints on risk assessment, response, and monitoring activities.
- Risk appetite and risk tolerance (e.g., acceptable levels and types of risks, and degree of risk uncertainty).
- Priorities and trade-offs (e.g., the relative importance of missions/business functions, trade-offs among different types of risk, and time frames in which the organization must address risk).

Assumptions identified during risk framing inform decisions and actions throughout the risk

---

<sup>20</sup> NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems & Organizations*, Apr 2015.

<sup>21</sup> The strategy must describe the way the organization will assess, respond, frame, and monitor risk.

<sup>22</sup> Information security risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence - NIST SP 800-39, *Managing Information Security Risk*, Mar 2011.

<sup>23</sup> NIST SP 800-12 Rev. 1, *An Introduction to Information Security*.

<sup>24</sup> The strategy must describe the way the organization will assess, respond to, and monitor risk.

management process.<sup>25</sup> After information security risk is framed, organizations should apply consistent methodologies to assess risks and determine appropriate risk responses. It is important to prioritize risk responses to support the agency's primary mission essential functions and to protect its critical systems and/or High Value Assets (HVAs). Risk monitoring is critical to verify risk responses are implemented and effective.

### **Privacy Risk**

The National Institute of Standards and Technology (NIST) Privacy Framework is designed to assist agencies and other organizations with managing privacy risk arising from data processing and strengthening privacy programs by enabling them to identify their ideal privacy outcomes and chart a path to reach those outcomes. Privacy risk management practices need to consider the full lifecycle of information, from creation, use and storage (including data at rest), through disposal. Taking a risk-based approach to privacy assists agencies in optimizing the development and use of innovative systems, products, and services while minimizing adverse consequences for individuals.<sup>26,27</sup>

### **Cyber Supply Chain Risk**

Supply Chain Risk Management is an increasing area of focus in agency ERM programs. Specific risks related to compromises in the supply chain for information technology and communication products and services, including dependencies on third parties intersecting with those products and services, have long been a point of concern in federal government.<sup>28</sup> Cyber Supply Chain Risk Management (C-SCRM) is a component of SCRM that refers to the potential for harm or compromise that arises as a result of cybersecurity risks from suppliers, their supply chains, and their products or services. As NIST notes, "managing cyber supply chain risks require ensuring the integrity, security, quality and resilience of the supply chain and its products and services."<sup>29</sup> As a result, cyber supply chain risks consider the broader threats and vulnerabilities of the products and services traversing the supply chain (i.e., counterfeits, unauthorized production, product tampering, thefts, etc.) as well as the threats and vulnerabilities to the supply chain itself. C-SCRM should be part of an enterprise-wide risk management approach and can be tailored for specific uses.<sup>30,31</sup> NIST recommends the use of C-SCRM methods and

---

<sup>25</sup> See NIST SP 800-30, Guide for Conducting Risk Assessments, Sept 2012.

<sup>26</sup> NIST Privacy Framework, A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0, Jan 2020.

<sup>27</sup> NIST Privacy Framework: An Overview, ITL Bulletin, Jun 2020.

<sup>28</sup> NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework), v1.1 Section 3.3, Apr 2018.

<sup>29</sup> NIST Cyber Supply Chain Risk Management: An Overview, Sept. 2021.

<sup>30</sup> NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems & Organizations, Apr 2015.

<sup>31</sup> NIST Cyber Supply Chain Risk Management Project, <https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management>.

advises that an effective enterprise-wide risk management defines risk tolerances to support supply chain decisions at all levels of the organization.<sup>32</sup>

## H. ERM Principles within Information Systems

Agency ERM programs emphasize those risks and opportunities that could have negative or positive impacts to the agency's reputation, its ability to achieve mission objectives, and the public trust in government. Information security, cybersecurity, privacy, and cyber supply chain risks are often considered domain-specific risk management practices and continue to be areas of focus in agency ERM programs. Managing these risks should be done in concert and coordination with each other and with agency ERM programs to critically inform top agency risks. An agency's ERM program needs to be dynamic and inclusive of all areas of risk including these risks mentioned above.

NIST establishes the information security, cybersecurity, privacy, and cyber supply chain risk management standards, requirements, and guidance for federal agencies. The Department of Homeland Security (DHS) and OMB partner to monitor the alignment of federal agency information security and cybersecurity programs with NIST standards and establish metrics for assessment of those programs.<sup>33</sup> NIST standards and guidance highlight key intersection points of how information security risk can impact organizational operations (i.e., mission, functions, image, and reputation) as one component of an agency's ERM program.<sup>34</sup> For example, failures in information security and cybersecurity risk management, or compromised personal information (privacy) can result in damage to reputation, unexpected costs, and the inability to execute mission essential functions. An agency level ERM program needs to be dynamic and inclusive of all areas of risk, which requires cooperation and integration across many business functions.

### Information Systems Risk Management and the Enterprise

Managing risk is a critical element of information systems management. The NIST Risk Management Framework (RMF) and recent guidance highlights the importance of linking risk management processes at the system level to those at the organization and enterprise levels.<sup>35,36</sup> Through recurring system assessments and authorizations and ongoing oversight, monitoring, and testing of system controls, risks can be integrated into discussions with management to ensure that decisions about risk response, including acceptance, are data-driven and timely. The effectiveness of these risk management processes can vary if an agency does not have a full grasp of the enterprise-level impact of risks accepted across multiple systems following RMF-based risk assessments. If risks are accepted at operational levels and not effectively communicated upward through the organization, then the agency's full exposure to information system risk will not be adequately understood and decisions on

---

<sup>32</sup> [NIST IR 8286 – Integrating Cybersecurity Risk Management with Enterprise Risk Management \(ERM\)](#), Oct 2020.

<sup>33</sup> [Inspector General Federal Information Security Modernization Act of 2014 \(FISMA\) Reporting Metrics Version 4.0](#), Apr 2020. DHS's Cybersecurity and Infrastructure Security Agency (CISA) runs the Continuous Diagnostics and Mitigation (CDM) Program to reduce cyber risk and provide visibility across the federal government, [www.cisa.gov](http://www.cisa.gov).

<sup>34</sup> NIST SP 800-39 and NIST IR 8286.

<sup>35</sup> NIST SP 800-37, Rev 2 and NIST IR 8286.

<sup>36</sup> Terms are further defined in Section C.

assigning resources to respond to system-level risks will remain misaligned to the magnitude of enterprise risk.

## Cybersecurity and Privacy Risk Management

The same concepts apply in managing cybersecurity and privacy risks within agencies.<sup>37</sup> The NIST Cybersecurity Framework (CSF), the NIST Privacy Framework, and the RMF are used in tandem to support communications about cybersecurity and privacy risk and results within organizations. At the enterprise level, agencies should be seeking to integrate cybersecurity and privacy risk management with agency ERM. One method to increase integration of cybersecurity and privacy risk within ERM is to use universally understood risk terms in communications. Chief Information Security Officers (CISOs) play a key role in connecting the lower levels of the organization to the agency ERM function using common language and tools, such as the cybersecurity risk register. This is a key tool that can enable translation of top cybersecurity risks to agency ERM functions.<sup>38</sup> Where agency cybersecurity programs are more advanced than privacy risk management, agencies should consider applying the same approaches and best practices described in this document for cybersecurity risk management to privacy risk management.

## Governance Structure and Risk Appetite Considerations

The governance structure of an enterprise can be designed to ensure that risk-based decisions are made at the appropriate levels. Traditionally, the “organization” has been defined as a multi-level entity – composed of a top level where governance and strategic decisions are made, a middle level where mission programs are managed, and a lower level where operations and information systems are managed.<sup>39,40</sup> More recently, the “enterprise” has been described as the pinnacle of the entity and the “organization” as the various business units within the enterprise. An “organization” can then describe any level or group within the agency below the “enterprise” or governance level.<sup>41</sup> (See Figure 2).

As part of an organization’s preparation to manage information security and privacy risks, the RMF describes the importance of assigning roles for risk management, enabling executive decision-making on risk appetite, and identifying the enterprise-level impacts of system risks. This can facilitate effective communication between senior leaders and executives at the organization and mission/business

---

<sup>37</sup> "...Cybersecurity risk management comprises the full range of activities undertaken to protect IT and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting IT and data, and to mitigate the impact of, respond to, and recover from incidents..." (E.O. 13800).

<sup>38</sup> As an example, the cybersecurity risk register is used to summarize risks at the operational level. Understanding agency ERM program criteria can help the CISO translate and escalate top risks. See NIST IR 8286.

<sup>39</sup> [NIST SP 800-39, Managing Information Security Risk](#), Section 2.1, Mar 2011.

<sup>40</sup> [NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations](#), Dec 2018.

<sup>41</sup> [NIST IR 8286, Integrating Cybersecurity and Enterprise Risk Management](#), Oct 2020.

process levels and system owners at the operational level.<sup>42</sup> Within most federal agencies, the Chief Information Officer (CIO) and/or the Chief Information Security Officer (CISO), holds the role of the Risk Executive function *in the information security and cybersecurity domains*. Similarly, the Senior Accountable Official for Privacy has agency-wide responsibility and accountability for the agency's *privacy* program. A complementary Risk Executive function often exists at the enterprise (agency) level in the form of a Chief Risk Officer, ERM Council or Risk Management Committee *to oversee enterprise risks*.<sup>43</sup> The agency ERM function needs to ensure that information security, cybersecurity and privacy risks can be normalized (translated using agency ERM rating criteria and terminology) to allow comparison with other types of enterprise risks. Agencies will benefit from ensuring that the lead risk executives within these functional domains and the agency ERM function partner closely.

An updated view of enterprise-wide risk management is represented in Figure 5. This view demonstrates the continuous influence of a top-down, bottom-up risk management strategy.<sup>44</sup> Risk appetite is defined at the enterprise level and then influences the parameters set at the operational level (risk tolerance).<sup>45</sup> At a systems level, this can reflect the amount of residual risk accepted following the implementation of risk response plans on identified system vulnerabilities. At the enterprise level, senior leaders working in consultation with the agency's ERM Council, Risk Management Committee, or other applicable governance structure overseeing enterprise risks need to understand whether the aggregate amount of risk accepted based on risk tolerance decisions at the system level is below, above, or in alignment with, their established risk appetite, and to understand the associated implications. To do this, risks need to be translated in terms of the impact to achieving mission objectives in non-technical terms (see [Appendix K – Use case 6](#)). This will help senior leaders make better informed decisions regarding allocation of resources for information security and cybersecurity risk mitigation in context of other risks faced by the agency.<sup>46</sup>

---

<sup>42</sup> NIST SP 800-37 Rev. 2 – See the “Prepare” step. The agency Senior Accountable Official for Risk Management (SAORM) is the head of the agency or equivalent who oversees the “Risk Executive” function. The Risk Executive function is “an individual or group within an organization that provides a comprehensive, organization-wide approach to risk management.”

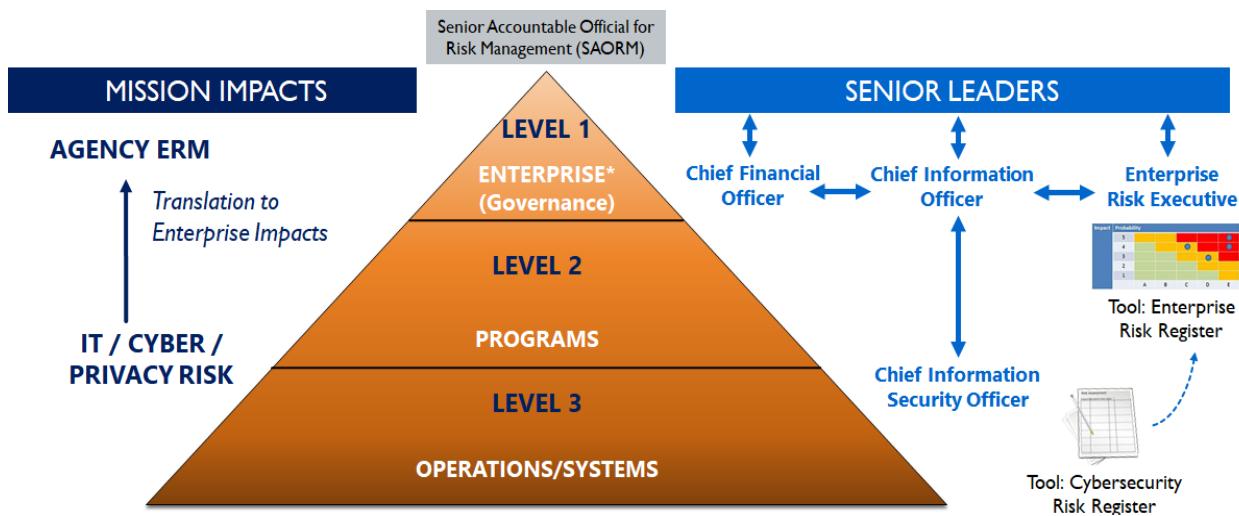
<sup>43</sup> In large, federated agencies, these roles and governance structures may be instituted at the sub-unit or organization level.

<sup>44</sup> Can be applied in information security and cybersecurity, or other settings.

<sup>45</sup> OMB A-123 defines risk appetite as the types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value, adopting the COSO definition.

<sup>46</sup> [OMB A-123](#) allows some discretion for agencies to establish risk tolerance at appropriate levels.

**Figure 5: Enterprise-wide Risk Management Approach with Horizontal and Vertical Communication**



#### Integration of OMB Circular No. A-123 and OMB Circular No. A-130 Requirements

As part of its revised policy in OMB Circular No. A-130 (OMB A-130) in 2016,<sup>47</sup> OMB established minimum requirements for federal information security, cybersecurity and privacy programs and linked these mechanisms to agency responsibilities under OMB A-123. These two circulars are related through their common emphasis on agency risk management and best practices, which include establishing risk management outcomes, effective governance, and communication. OMB A-123 requires agencies to develop an Agency Risk Profile<sup>48</sup> on an annual basis to identify and analyze the risks an agency faces toward achieving its strategic objectives. The risk profile facilitates open and candid conversations about risks facing an organization at all levels and enables a portfolio view of risk. It 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. It assists in facilitating a determination around the aggregate level and types of risk the agency and its management are willing to accept to achieve its strategic objectives. CISOs and Risk Executives from business functions should consider if or how cybersecurity risks can impact programs and operations and, conversely, how risks from non-IT areas may have cybersecurity risk implications. The products and artifacts resulting from an agency's OMB A-130 activities and external audits can provide additional insight on these intersection points. For example, systems level assessments, OMB A-123 assessments and the annual Federal Information Security Management Act (FISMA) audit, should inform risk registers and the Federal Managers Financial Integrity Act (FMFIA) annual statement of assurance. As a best practice, agencies should define and utilize common enterprise-level risk criteria to determine whether information security, cybersecurity, or privacy risks should escalate to agency level ERM risk registers.

#### Establishing Critical Information Systems and High Value Assets (HVAs)

<sup>47</sup> OMB A-130 Appendix I describes agency responsibilities for protecting federal information resources and for compliance with the Privacy Act of 1974.

<sup>48</sup> OMB A-123 defines a risk profile as a thoughtful analysis of the risks an agency faces toward achieving its strategic objectives and arising from its activities and operations.

Identifying HVAs and mission critical assets is an important way to prioritize attention for management of information security and cybersecurity risks. If these systems are vulnerable, then the mission of the agency will be at risk. Key considerations include the degree to which the system supports the agency's primary mission essential functions; whether it has a high volume of sensitive or protected information, such as controlled unclassified information, personally identifiable information, or regulated information, and the nature and scale of impact to the public, federal enterprise essential functions, national security, or the economy if a compromise occurred. Agencies are expected to identify their most critical functions, information and data and consider how these critical functions support or are central to their organization's mission responsibilities.<sup>49,50</sup> Facilitating integrated risk assessment and communication with impacted parties is a key element of an effective ERM program.

## I. Approaches to Enterprise Risk Management, Information Security, and Cybersecurity Risk Management Integration

---

### Cyber-ERM Integration Outcomes

- Provides a disciplined approach to support leadership understanding and awareness of organizational risks and interdependencies and the management efforts to address them.
  - Leads to improved decision-making by providing a framework for value-added discussions, decision points, and tradeoffs for leadership to deliberately consider enterprise risks and opportunities.
  - Reinforces program management best practices by fostering open and candid conversations about accepting an appropriate level of risk, based on risk appetite and risk tolerance, to achieve desired outcomes.
  - Allows agencies to make deliberate choices at different levels of the organization, allowing them to pursue more "value creation" in programs and projects, in addition to the traditional mindset of "value protection."
  - Offers leadership a strategic mindset and organizational capability which support the tracking and mitigation of unprecedented occurrences that impact an agency's mission and reputation, thus enhancing transparency and accountability for delivering results to the public.
- 

### Value Proposition

Effective ERM is a shared responsibility within an organization, from executive leadership to service delivery staff. Integration of information security and cybersecurity risk management within an agency ERM program requires a culture that reflects the importance of how practicing ERM supports the agency's mission. ERM enables cross-functional discussions to identify, manage, and communicate

---

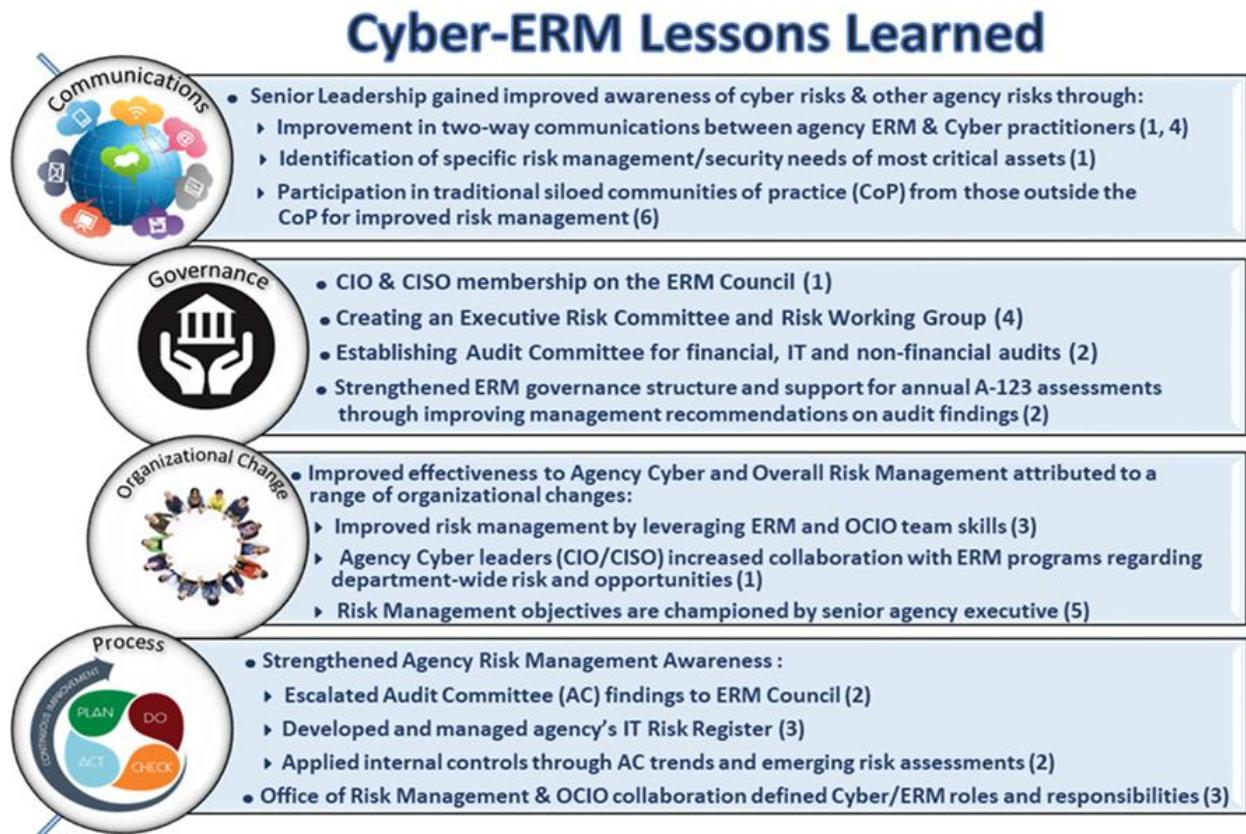
<sup>49</sup> Other examples include intellectual property, protected health information, and financial information.

<sup>50</sup> OMB and DHS release federal guidance and requirements on HVAs; [OMB M-19-03](#) advises federal agencies to take a strategic enterprise-wide view of risk when identifying HVAs. Also see DHS Binding Operational Directive ([BOD](#)) 18-02 and Federal Continuity Directive 1 and [Directive 2](#).

potential enterprise-level impacts of cybersecurity risks and the relationship of cybersecurity risks to other enterprise risks within an agency's risk profile. This will allow prioritization based on likelihood and impact, which results in better utilization of limited resources.

Per agency experience, it is an effective ERM practice to include the agency CIO and/or agency CISO on the agency's Risk Management Council or similar ERM governance body for effective integration with ERM.<sup>51</sup> Figure 6 below summarizes key lessons learned from agency approaches to integrating cybersecurity and agency ERM. Appendix K provides the detailed agency case studies, and the numbers below indicate the case study demonstrating each lesson learned.

**Figure 6: Summary of Cyber-ERM Integration Lessons Learned**



### Quantitative and Qualitative Cyber Risk Management Frameworks and Methodologies

The NIST CSF offers a flexible way for organizations to address and track cybersecurity risks and program maturity, designed to strengthen cybersecurity risk management practices, regardless of an organization's size and maturity level.<sup>52,53</sup> Agencies that utilize a blended approach by incorporating

<sup>51</sup> CIO and CISO responsibilities are outlined in FISMA 2014, Sec 3554 (a)(3)(A).

<sup>52</sup> Mandated by Executive Order 13800.

<sup>53</sup> The NIST CSF should be used in conjunction with an additional security framework, such as the RMF – utilizing the CSF alone can lead to assessments where weaknesses go undetected, which can create a false sense of security posture or risk exposure.

qualitative and quantitative models can strengthen their existing risk analysis processes, complementing the CSF and Risk Management Framework methodologies (see [Appendix L](#)).<sup>54</sup> Agencies can consider current data sources and familiarity with existing qualitative risk management processes and combine these with quantitative approaches to improve their overall risk awareness and create a consistent, repeatable, and more precise practice of risk management to better support and inform risk decisions.

### **Existing Frameworks and Methodologies for Integration with Enterprise Risk Management**

CISOs can derive benefit from discussing internal and external risks with system owners, stakeholders, and management utilizing common terms captured within the NIST CSF. Similarly, the NIST Privacy Framework assists organizations in determining where their greatest exposures are with respect to data processing by performing a privacy risk assessment. At the enterprise level, both threat risks and opportunity risks need to be discussed to allow strategic decision-making based on impacts to mission.<sup>55</sup>,<sup>56</sup> Organizations need to apply risk assessment models to allow for innovative practices or system changes deemed beneficial to the organization (upside risk). As previously written, the same concepts apply to cyber supply chain risk.

### **Improving Communication on Risks with Decision-Makers**

Effective cybersecurity risk management at the enterprise level ensures senior management and decision makers at all levels of the organization have visibility into the cyber risks that exist at their level and below. Because information and communications technology support many of an organization's business processes designed to support mission execution, cybersecurity risk management has become a key pillar in agency-level ERM programs. Threats to information systems, data, and assets, can and do have outsized impacts to an organization's capability to accomplish its mission. As such, the Chief Risk Officer (CRO), or equivalent, should be included in timely discussions on cybersecurity risks so that the impact of the risk to the enterprise can be evaluated. The CRO, working with the cybersecurity team, can identify the potential impacts on strategic goals and objectives of the organization. To assist in ensuring cybersecurity risks are reported to senior management regularly and in a timely fashion, the reporting responsibilities of key personnel should be outlined and common criteria for escalation should be defined. Examples of these can be found in [Appendix M](#) and a sample reporting flow can be found in [Appendix N](#).

### **Cybersecurity Risk Management Reporting**

Appropriate communication of risk and determinations of risk to information systems, as conducted by cybersecurity staff, is essential to safeguarding information and ensuring effective operations. Agency cybersecurity risk management programs rely on inputs from several sources to determine whether the risk exceeds the enterprise's risk appetite and operations-level risk tolerances. Many of the known risks are derived from the results of existing work processes, allowing cybersecurity professionals to focus on securing assets and systems. While the main data source for risk metrics is gathered through Information Security Continuous Monitoring (ISCM), Plans of Action and Milestones (POA&Ms), and Security Assessments, other sources can be used as necessary to obtain a complete picture of the risk

---

<sup>54</sup> [NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations](#), Dec 2018.

<sup>55</sup> Risk Profiles should consider both positive (opportunities) and negative (threats) sources of uncertainty. See OMB A-123, Section II.B.

<sup>56</sup> Also see: [NIST IR 8170, Integrating Cybersecurity and Enterprise Risk Management](#), March 2020.

landscape, such as: analysis of HVA or other critical systems, data feeds from DHS tools, US-Cyber Emergency Readiness Team notifications, information from FISMA audits and reporting, Government Accountability Office (GAO), or Office of Inspector General (OIG) findings, DHS vulnerability assessments, and helpdesk reporting of phishing attempts, among many others.<sup>57</sup>

An analysis of the risk's likelihood and its potential impact must be conducted initially by cybersecurity staff who will use established risk assessment methodologies applicable at the system or business process level to determine severity, typically captured in a cybersecurity risk register and heat map.<sup>58</sup> Once in hand, the CISO, along with other personnel, will assess the risks against escalation criteria, or critical impact criteria, that will help determine what level of reporting is required for top risks. The CISO will use internal and external information to assess risks and to review trends and patterns. The information should ideally be gathered and reported in a systematic way using a standardized format. A tiered reporting approach can be defined and used to determine which risks, based on severity at the systems/operations level and potential for impact at the enterprise level, should be reported to senior management and to the CRO. This is an important integration point with agency ERM functions.

## J. Addressing Confusion in FISMA Audits

### Background on FISMA Audits

The Federal Information Security Modernization Act of 2014 (FISMA) requires each agency Inspector General (IG), or an independent external auditor, to conduct an annual independent evaluation to determine the effectiveness of the information security program and practices of its respective agency. IGs and external auditors assess the effectiveness of information security programs using a maturity model with several reporting metrics covering various information security topics, including risk management.

Additionally, IGs and external auditors have also been required to address certain ERM-related metrics during FISMA audits.<sup>59</sup> In doing so, some agencies have experienced that (a) their agency ERM programs and capabilities have become an outsized focus of FISMA audits in comparison to their information security program and cybersecurity risk management practices; (b) ERM-related FISMA audit conclusions, results, findings, and recommendations do not reflect the flexible and non-compulsory nature of most ERM-related criteria; and (c) auditor expectations for the maturity of processes integrating ERM, information security programs, and cybersecurity risk management practices may be more compulsory than actually prescribed historically, given the absence of federal standards and consistent frameworks on integrating ERM with information security programs and cybersecurity risk management practices.<sup>60</sup>

---

<sup>57</sup> The DHS Continuous Diagnostics and Mitigation (CDM) program provides federal agencies with several automated tools to support near real-time data collection, analysis, and reporting.

<sup>58</sup> See [NIST SP 800-30, Guide to Conducting Risk Assessments](#) and the [NIST Privacy Risk Assessment Methodology](#) for privacy.

<sup>59</sup> The IG FISMA Reporting Metrics are developed as a collaborative effort amongst OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in consultation with the Federal Chief Information Officer (CIO) Council and other stakeholders.

<sup>60</sup> NIST IR 8170 and NIST IR 8286 provide new guidance on integration of cybersecurity and ERM.

## Differentiating FISMA Audits from Agency ERM

Agency ERM programs go well beyond the boundaries of the agency information security programs and the risk management practices that are within the scope of FISMA audits. Accordingly, it is important for agencies that FISMA audits remain focused on information security programs and practices, rather than serving as audits of agency ERM programs. While agency ERM programs can enhance risk management and communications across functional areas, including information security programs, an assessment of an agency's ERM program maturity and effectiveness should focus on effectiveness of risk management practices within the functional domain of information security and its effectiveness in integrating with agency ERM programs.<sup>61</sup>

Within DHS's annual reporting metrics for the IG and external auditors, references are sometimes made to key ERM-related criteria, such as OMB A-123 and this Playbook. However, the content of this Playbook should not be considered prescriptive or set the standard for audits or other compliance reviews.<sup>62</sup> OMB A-123 and the Playbook emphasize flexibility in implementing agency alignment with suggested criteria and characteristics of agency ERM programs. Similarly, other key ERM-related criteria published by non-federal entities, such as COSO in its *Enterprise Risk Management—Integrating with Strategy and Performance* framework, highlight its intent for use as guidance versus as policy.<sup>63</sup>

In the course of FISMA audits, it is helpful to agencies when auditors are well-versed on the different criteria and objectives for information security risk management at lower levels of the organization versus agency ERM at the highest level. It is also useful when auditors have discussions with agencies about how agency ERM and information security risk management programs interact with each other and how auditors plan to apply various criteria related to these programs at the respective organizational levels. These discussions can offer agencies and their FISMA auditors a very clear understanding from the outset of the audits how agencies will be measured and will lead to more valuable outcomes.

---

<sup>61</sup> For example, the ERM governance structures that enable communication and the frequency and method of communications across these functional areas could be relevant.

<sup>62</sup> [Inspector General Federal Information Security Modernization Act of 2014 \(FISMA\) Reporting Metrics Version 4.0](#), April 2020. Of 59 FISMA reporting metrics for which the assignment of a maturity rating is required, four (seven percent) include a reference to OMB A-123 and/or the initial version of this Playbook. These four metrics fall within one of eight sub-domains addressed by the metric: Risk Management.

<sup>63</sup> U.S. federal agencies are not required to apply the [COSO ERM framework](#) when implementing ERM, but the COSO Framework does provide useful guidance, and is sometimes referenced in OIG reports as audit criteria. The GAO "Green Book" or [Standards for Internal Control in the Federal Government](#) also address Risk Management practices as part of the overall control environment.

# X. 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.

## Table of Contents

X. Appendices .....	61
A. Risk Types .....	62
1. Credit Risk .....	64
B. ERM Governance/ Culture.....	65
1. Organization Charts .....	65
2. Position Descriptions .....	72
3. Risk Committee Charters .....	88
4. Facilitating an ERM Culture Conversation .....	91
5. Implementation Plans.....	93
C. ERM Frameworks.....	95
D. Maturity Models.....	100
E. Risk Assessment.....	108
1. Establishing Context .....	108
2. Risk assessments and the ERM Process.....	109
F. Risk Profile.....	110
1. Key Questions to Help Develop a Risk Profile .....	110
2. Templates .....	111
3. Risk Assessment Tools .....	118
G. Risk Reporting and Monitoring .....	132
1. Dashboards .....	132
2. Monitoring .....	134
H. Linking Risk and Performance .....	136
I. Risk Appetite .....	138
J. Glossary .....	139
K. Special Chapter: Cyber – ERM Integration Use Cases .....	147
L. Examples of Qualitative and Quantitative Risk Analysis Approaches.....	152
M. Examples of Roles and Responsibilities of Key Personnel for Effective Information Security and	

Cybersecurity Risk Management .....	153
N. Example of a Risk Communication Process Flow .....	154
O. References and Resources .....	155
P. Agency Acknowledgements.....	156

## A. Risk Types

Risk Type	Risk Description
<b>Compliance Risk</b>	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.
<b>Credit Program Risk</b>	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.
<b>Cyber Information Security Risk</b>	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.
<b>Financial Risk</b>	Risk that could result in a negative impact to the agency (waste or loss of funds/assets).
<b>Legal Risk</b>	Risk associated with legal or regulatory actions and agency's capacity to consummate important transactions, enforce contractual agreements, or meet compliance and ethical requirements.
<b>Legislative Risk</b>	Risk that legislation could significantly alter the mission (funding, customer base, level of resources, services, and products) of the agency.
<b>Operational Risk</b>	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.

Risk Type	Risk Description
<b>Political Risk</b>	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.
<b>Reporting Risk</b>	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.
<b>Reputational Risk</b>	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.
<b>Strategic Risk</b>	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 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.

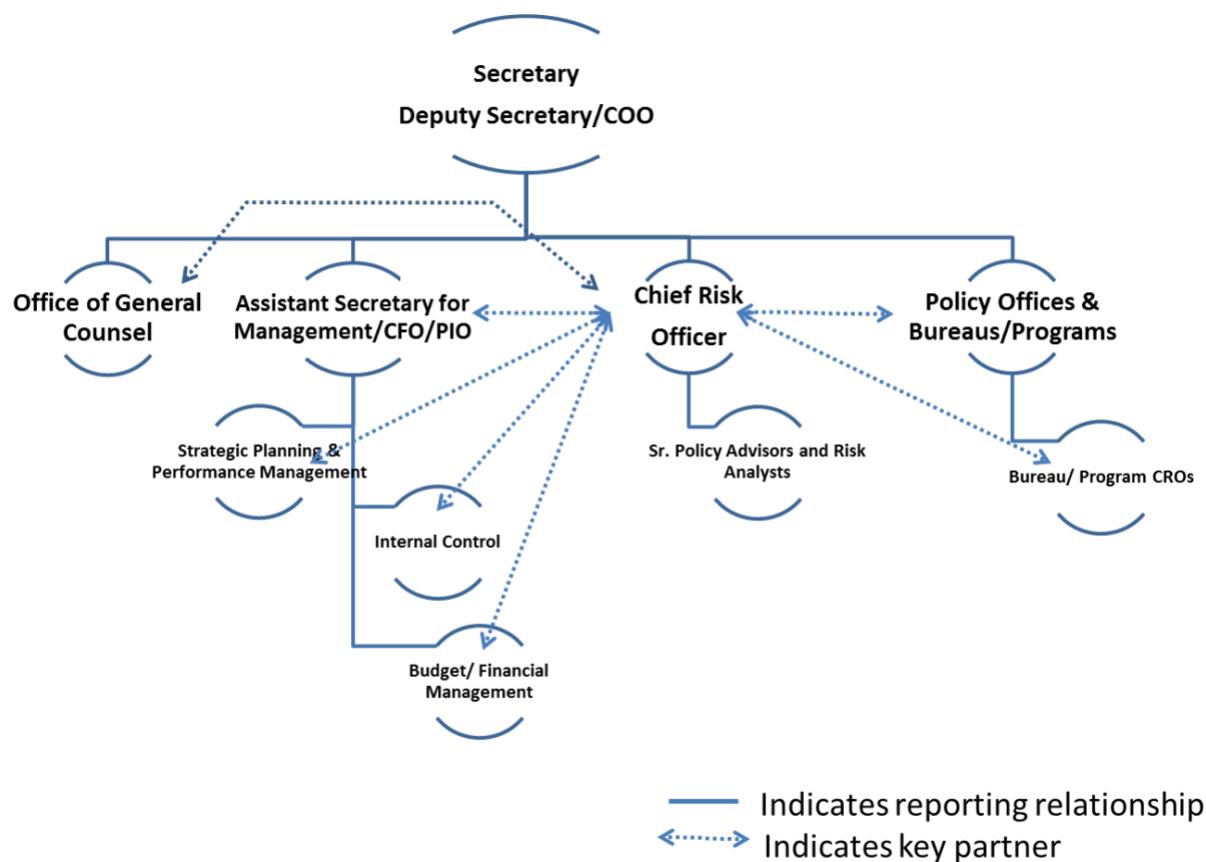
Additional challenges faced by federal agencies in implementing credit programs are the increased administrative burden and operational risks associated with running credit programs compared with other forms of Federal assistance. Agencies require robust management and oversight structures to ensure 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 OMB A-129, "Policies for Federal Credit Programs and Non-Tax Receivables," 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. Enterprise Risk Management Governance and Culture

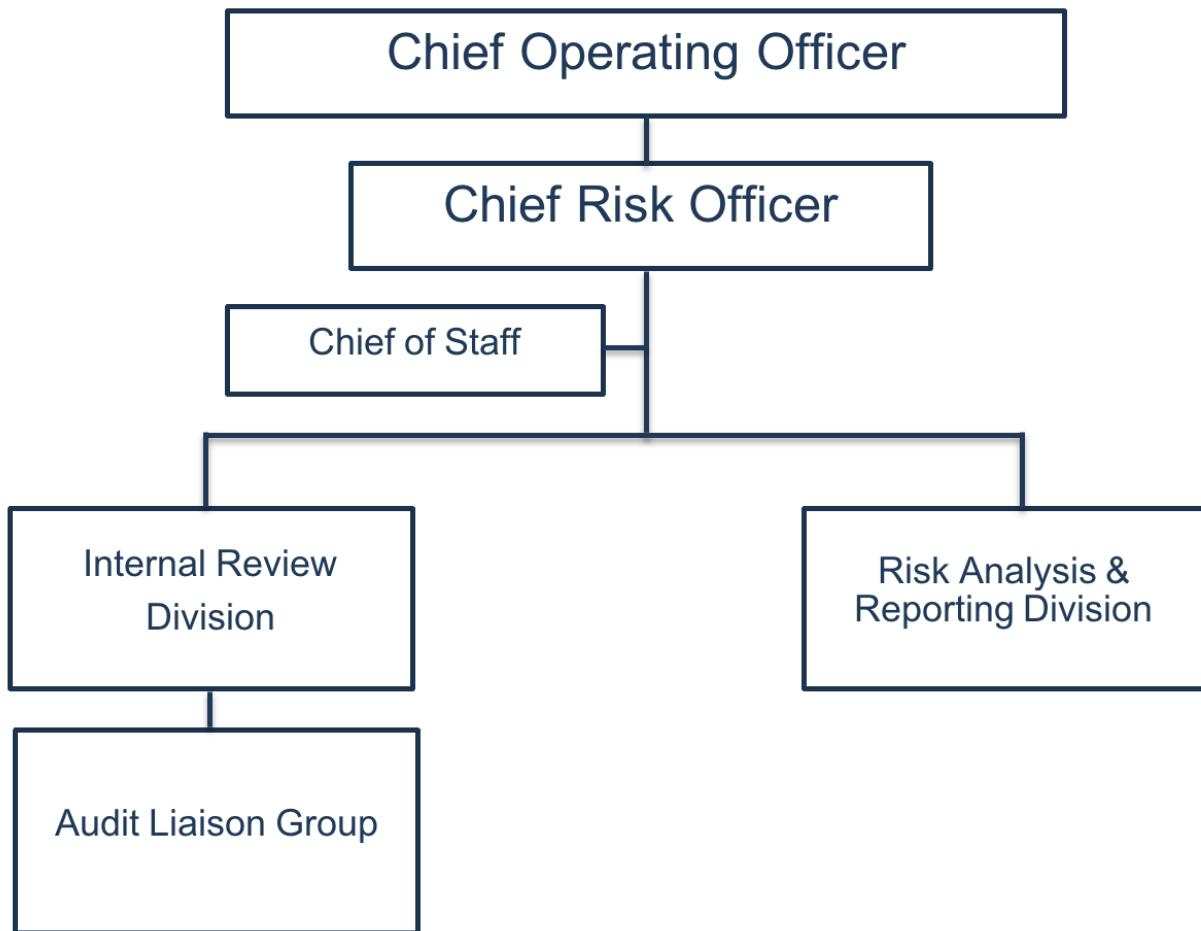
### 1. Organization Charts

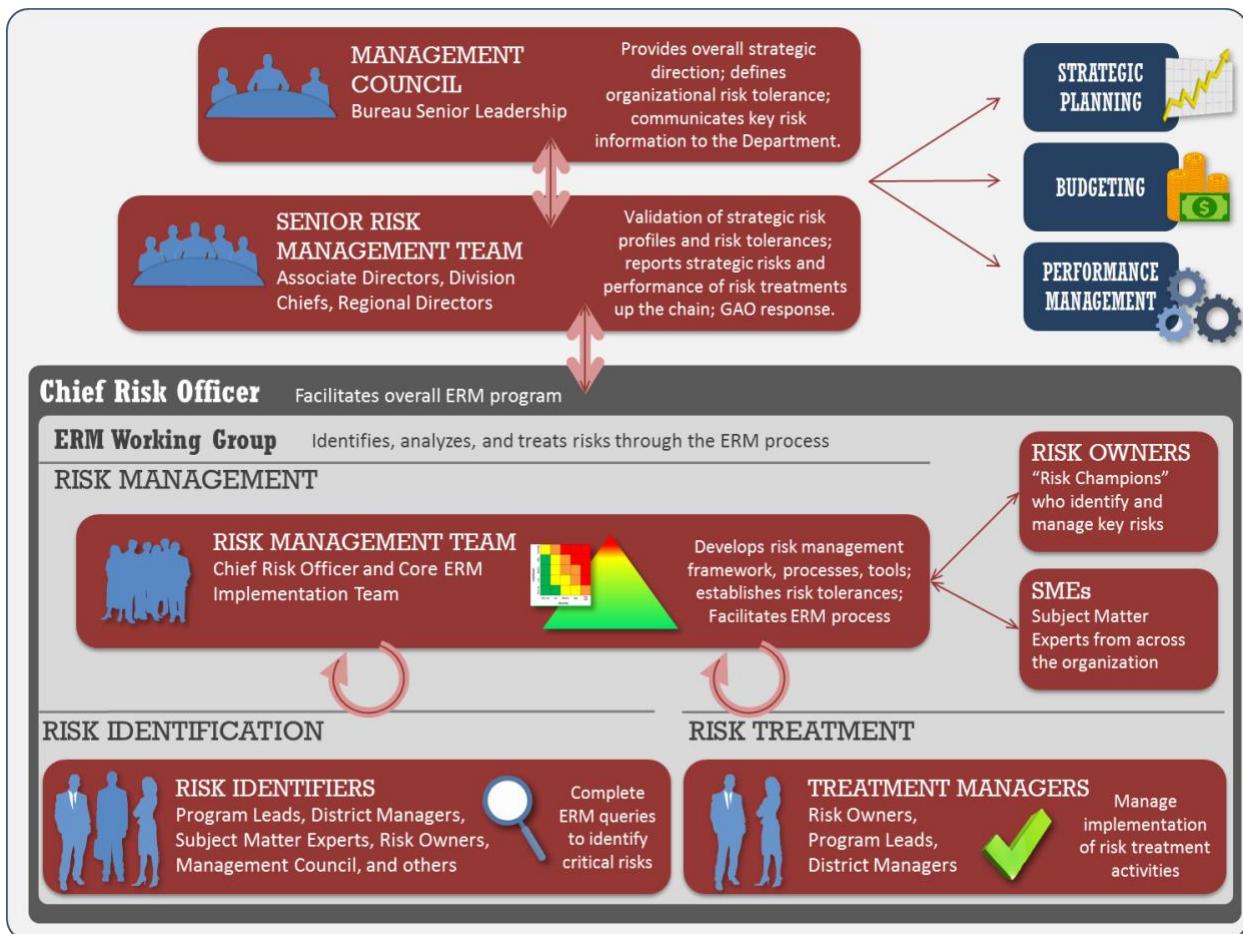
#### a. Relational Organization Chart in Agency with CRO Function at Senior Level (Example)



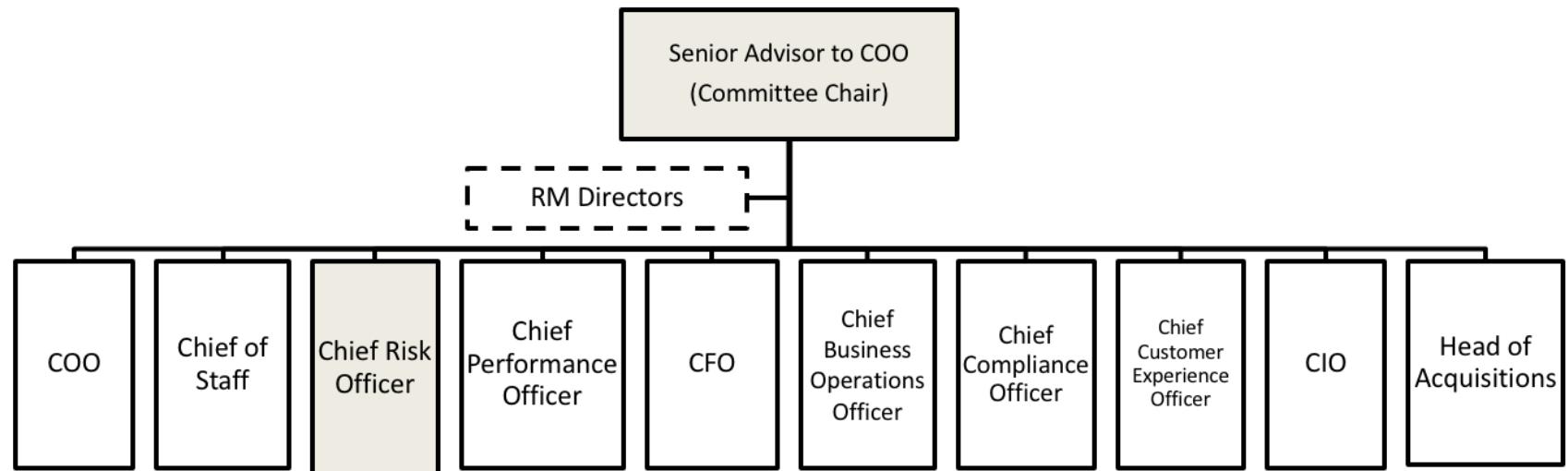
**b. Relational Organization Chart in Bureau with CRO Function at Senior Level (Example)**

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



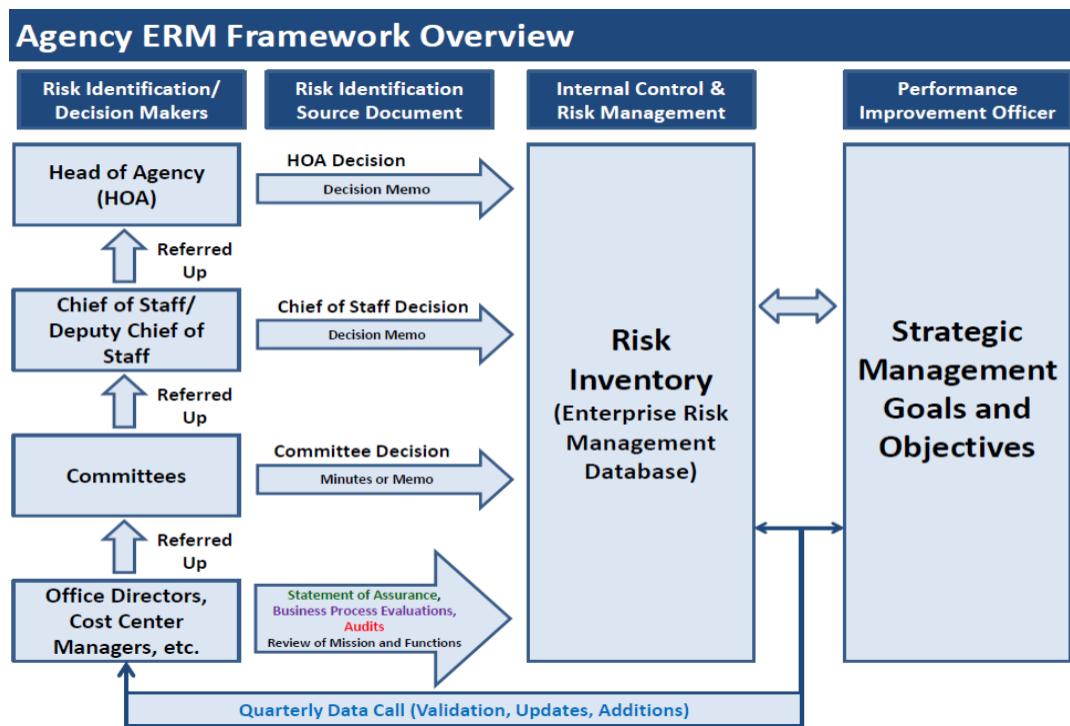


*c. Risk Management Committee (Example)*



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

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



**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	<ol style="list-style-type: none"> <li>1. Quarterly Risk Reporting (data call to coincide with Performance Measurement Goal Reporting)</li> <li>2. Statement of Assurance Risk Assessment</li> <li>3. Business Process Evaluations</li> <li>4. Audits</li> <li>5. Review of Mission and Functions Statement</li> </ol>	<ol style="list-style-type: none"> <li>1. Quarterly Performance Summaries and Risk Assessment Input and Tracking Template</li> <li>2. Statement of Assurance Template/Letter</li> <li>3. Internal Control Test Plan</li> <li>4. Evaluation/Audit Findings</li> <li>5. Mission and Functions Statement</li> </ol>	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.

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

Role	Responsibilities
Standing Management Committees, for example: <ul style="list-style-type: none"> <li>• Executive Management Council (EMC)</li> <li>• Risk Management Council (RMC)</li> <li>• Senior Assessment Team (SAT)</li> <li>• Audit Committee</li> </ul>	<ul style="list-style-type: none"> <li>• 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)</li> <li>• 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</li> <li>• 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</li> </ul>
Chief Operating Officer (COO)	<ul style="list-style-type: none"> <li>• Identify and coordinate actions that improve results, enhance efficiency, manage risks, and reduce waste</li> <li>• Incorporate risk discussions in the strategic planning and performance management processes</li> <li>• Track risks</li> <li>• Facilitates discussions on risk prioritization for the agency</li> <li>• Analyzes the impact of specific risk to the agency</li> <li>• Coordinates the development of risk response plans where and if applicable</li> <li>• Works with the EMC, ICRM, PIO, and Committee chairs and members to present risks to the head of the agency</li> </ul>
Chief of Staff and Deputy Chief of Staff	<ul style="list-style-type: none"> <li>• 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</li> </ul>
Internal Control and Risk Management Division (ICRM)	<ul style="list-style-type: none"> <li>• Provides guidance to help the agency develop a common vision, definition, and strategy for managing risk</li> <li>• Facilitates the development of a common language and clarifies terminology to enable constructive discussions</li> <li>• Provides guidance to establish and implement an ERM framework that facilitates the use of the risk cycle approach</li> <li>• Works with the CAO, CFO, CIO, COO, GC, PIO, and Office of Budget to track and report organizational risks</li> <li>• Monitor and validate risks identified within the ERM Database</li> </ul>
Performance Improvement Officer (PIO)	<ul style="list-style-type: none"> <li>• Promotes the application and execution of risk management practices in the strategic planning, performance planning and reporting, and strategic review processes</li> </ul>
Office of Budget	<ul style="list-style-type: none"> <li>• Incorporates risk management practices in the budget formulation and execution processes</li> </ul>
Office Directors/Goal Leaders/Cost Center Managers	<ul style="list-style-type: none"> <li>• For their areas of responsibilities:           <ul style="list-style-type: none"> <li>○ Conduct risk analysis:</li> </ul> </li> </ul>

Role	Responsibilities
	<ul style="list-style-type: none"> <li>▪ Description of risk</li> <li>▪ Annual Performance Plan Objective (if applicable)</li> <li>▪ Related Project or Function</li> <li>▪ Risk Treatment Category and Description</li> <li>▪ Resources Required and Cost</li> <li>▪ Probability of Occurrence of Identified Risk</li> <li>▪ Impact of Identified Risk</li> <li>▪ Type of Risk</li> <li>• Consult with ICRM as needed</li> <li>• Document and validate risks using the Enterprise Risk Management Database</li> <li>• Present risk analysis to the appropriate committee(s)</li> </ul>

## **2. Position Descriptions**

Creating ERM positions takes time and careful thought. Start by identifying why your organization, group, or team needs additional personnel. Part of the analysis should include a consideration of the current workload of employees, projections of future work efforts, and succession planning.

Questions to consider:

- Would it be better to create a stand-alone group that only has responsibility for implementing and managing ERM for the subordinate, component, and/or at the headquarters/department-level?
- Should ERM responsibilities be added to current functions that have some connection to risk in your agency? If so, will there be sufficient time and effort to conduct ERM responsibilities fully?
- Are there new initiatives or functions your agency is absorbing that you are creating a new section to manage? Would ERM fit there?
- Where will ERM have its best opportunity to flourish and best help the agency meet its mission?
- What justifies creating a new role/position in your organization?
- Are people increasingly overworked and stressed, because of the volume of tasks they must complete?

Alternatively, perhaps your projections for the next year show that initiatives and restructuring, will dramatically increase the workload and the ability to manage certain initiatives have become increasing difficult, you don't have a sufficient size team and skillset in place to handle the extra workload.

- **Consistent work overload** – The main indicator that people need extra help is that they are consistently overloaded with tasks and projects. If they work hard and manage their time effectively, then adding additional personnel will increase productivity as well as reduce stress.
- **Regular use of contractors** – Are you reliant on outsourcing this function? Be careful to avoid using contractors to assist with inherently governmental functions (see the Federal Acquisition Regulation, Section 7.503). This could mean that you need to establish and staff permanent, government position(s).<sup>64</sup>

### **Developing ERM criteria for Position Descriptions**

Position descriptions that include a summary of the ERM tasks and duties assigned to a position are critical to the execution of enterprise risk management efforts, and recruitment of the best-qualified individual(s) to fill this demanding role at the agency. They are based on objective information obtained through job analysis, an understanding of the competencies and skills required to accomplish needed tasks, and the needs of the organization to produce work.

To create and/or use a current ERM position description in your agency, it is helpful to keep in mind your agency's culture, reporting structure, and skills needed to effectively implement and/or manage ERM. If you are creating a job description, from scratch, either consider a current job analysis for ERM

---

<sup>64</sup> However, it is important to consider the pros and cons of contracted assistance, to include cost, flexibility, limits of support and potential personnel turnover.

and/or examples of recent ERM positions filled in the federal government. In any event, ensure that the position includes the essential ERM functions of the job and what minimum requirements are necessary to successfully perform the assigned functions to include: a description of the work, details the required tasks, knowledge, skills, abilities, responsibilities, and reporting structure.

Further, as the agency's goals and objectives change over time, it may be necessary to revise the ERM position to reflect changes in the organizational structure that will affect what really needs to be accomplished by the position.<sup>65</sup>

### **Enterprise Risk Management Practitioner competencies**

The following are examples of possible competencies that an agency may wish to have in its ERM team. This is not an exhaustive list or a list that must be used for every agency. Agencies should again, decide what works for them, where the positions will be in the organization and what the main goal of the position will be.

#### **General Competencies**

Accountability	Legal, Government, and Jurisprudence
Attention to Detail	Oral Communication/Listening
Coaching/Teaching	Partnering
Conflict Management	Planning and Evaluating
Creative Thinking	Political Savvy
Customer Service	Problem Solving
Decision Making	Reading Comprehension
External Awareness	Reasoning
Flexibility	Fiscal Stewardship
Influencing/Negotiating	Strategic Thinking
Information Management	Team Building
Integrity/Honesty	Teamwork
Interpersonal Skills	Technical Credibility
Leadership	Technology Application
	Written Communication

---

<sup>65</sup> Job descriptions must be accurate to meet the needs of those workplace responsibilities listed. While they are not meant to be so detailed in the exact number of tasks performed or every possible scenario that an employee may face in their job, they should include the general scope and level of the work to be performed.

## Technical Competencies

Business Intelligence	Process Improvement
Change Management	Project Management
Compliance	Program Evaluation
Correspondence Management and Action Staffing	Program Management
Cost-Benefit Analysis	Portfolio Management
Data Mining, Analysis, and Visualization	Quality Assurance
Decision Support	Risk Analysis
Expert Elicitation	Risk Exposure Analysis
Internal Controls	Root Cause Analysis
Knowledge Management	Stakeholder Management
Entity-level planning, programming, budgeting, and execution	Strategic Foresight
Organizational Design and Culture	Strategic Management
Outreach and Public Affairs	Strategic Planning
Performance Management	

**Cross-Functional Knowledge.** Experience in one or more of any operations or management functions/disciplines may be helpful for an ERM practitioner. These can include:

- Human resource and workforce management
- Financial management
- Financial services
- Credit programs or policy
- Acquisition management (i.e., science & technology, engineering, Research, Development, Testing, and Evaluation (RDT&E), procurement, contracting)
- Cybersecurity
- Sustainment management (logistics and supply chain)
- Information technology, business systems, data management
- Real property management
- Community services
- Safety and security management
- Mission assurance
- Information and records management and privacy policy, etc.
- Law enforcement and legal environment
- National security
- Programmatic knowledge

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

Chief Risk Officer (CRO)
<b>Introduction</b> <p>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].</p> <p>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.</p> <p>The CRO will provide executive-level management, leadership, direction, and oversight to the ORM and expertise to the [AGENCY] by identifying and advising on risk response 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.</p> <p>Assignments are complex, sensitive, and wide reaching in scope.</p>
<b>Duties and Responsibilities</b> <ul style="list-style-type: none"><li>• 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].</li><li>• 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.</li><li>• 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.</li><li>• Promotes a best-practice risk-management culture at the [AGENCY].</li><li>• Formulates and plans strategic and operational direction and expertise to the Office of Risk Management. Hires and supervises the Office's professional and support staff and promotes</li></ul>

### **Chief Risk Officer (CRO)**

the career development of each member of the staff. Provides 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, managing risks, determining, measuring, 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 the broad policy objectives of the [AGENCY] are carried out.

### **Job Competencies (The full range of competencies for the occupational series is provided for**

## Chief Risk Officer (CRO)

### 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, appraised, 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-in-class 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

### **Chief Risk Officer (CRO)**

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, 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 response 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 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	
<b>Introduction</b>	
<p>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.</p>	
<b>Major Duties</b>	
<ul style="list-style-type: none"><li>• Directs the implementation of agency's Enterprise Risk Management (ERM) Program.</li><li>• Implements strategies and provides guidance for improving risk management practices across the organization.</li><li>• Manages staff of Risk and 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 and maintenance of ERMG's Risk Tracking System (RTS) and other data initiatives and risk analyses supporting the goals of the agency and ERMG.</li><li>• Directs and develops plans for project teams or other groups to complete projects, studies, and risk assessments.</li><li>• 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.</li><li>• Provides day to day oversight and technical direction to contractors supporting the agency's ERM Program and other ERMG initiatives.</li><li>• Develops, analyzes, and evaluates new or modified program and management policies, regulations, goals, or objectives.</li><li>• Develops procedures and systems for assessing the effectiveness of programs and management processes.</li></ul>	
<b>Factor Levels</b>	
FACTOR 1 KNOWLEDGE REQUIRED Level 1–8 1550 points	
<ul style="list-style-type: none"><li>• 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.</li><li>• Knowledge of a comprehensive range of administrative laws, policies, regulations, and precedents applicable to the administration of one or more programs.</li><li>• 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.</li><li>• Knowledge of relationships with other programs and key administrative support functions within the agency or other agencies.</li><li>• Knowledge of advanced risk management and analytical practices, standards, and procedures.</li></ul>	

### **Director, Risk Analysis and Reporting**

- 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.

#### **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.

### **Director, Risk Analysis and Reporting**

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**

- Develops and maintains good working relationships with program, Departmental and external management and staff, represents ERMG and 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 and internal control weaknesses to agency programs.
- Monitors the execution of corrective action plans implemented to address audit and risk recommendations and reports on their effectiveness and value.
- Develops analytical and comparative risk reports for monthly, quarterly, and 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 Risk Analyst (Financial Agency) Position Description (OFFICE OF RISK MANAGEMENT) (Example)**

Senior Policy Advisor
<b>Introduction</b> <p>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.</p> <p>This position will serve as an expert specialist on a wide range of risk management matters and provide assistance in identifying and advising on risk response 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.</p>
<b>Major Duties and Responsibilities</b> <p>Under the general direction of the Chief Risk Officer, the Senior Policy Advisor shall:</p> <ul style="list-style-type: none"><li>• Plan, develop, recommend, coordinate, and implement risk management policies and strategies, as well as design management techniques to achieve risk management goals.</li><li>• Compare existing [AGENCY] program-level risk management practices against public and private sector (best practices) to propose and implement improvements as needed.</li><li>• Review existing program-level risk reporting, and work to enhance risk reporting where necessary.</li><li>• Develop [AGENCY]-wide risk monitoring reports, including detailed risk assessments.</li><li>• 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.</li><li>• Summarize findings and research in written products of various types, including tables, charts, short summaries, as well as longer analytical policy memos and reports.</li><li>• Conduct complex and authoritative research relating to proposals that affect the financial exposure of [AGENCY] programs.</li><li>• 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.</li><li>• Prepare responses to Congressional, press or other public inquiries.</li><li>• Coordinate with senior officials at the Office of Management and Budget and other Federal agencies to effectively assess and manage risks, and ensure that applicable OMB guidelines, directives, and standards are effectively met by [AGENCY] programs.</li><li>• Maintain strong working relationships and ongoing lines of communication with officers and other staff members.</li><li>• Promote a strong culture of risk management.</li><li>• Provide guidance to junior-level staff as needed.</li><li>• Perform other duties as assigned.</li></ul>

## Senior Policy Advisor

### **Factor Levels**

#### **FACTOR 1: KNOWLEDGE REQUIRED BY THE POSITION (1–8 1550 Points)**

- 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,

## **Senior Policy Advisor**

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 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.
- (3) Maintain PIV credential eligibility during their service with the [AGENCY].

*e. Senior Risk Analyst Position Description (Example)*

Senior Risk Analyst	
<b>Introduction</b>	
<p>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.</p>	
<b>Major Duties and Responsibilities</b>	
<ul style="list-style-type: none"><li>• Directs and develops plans for project teams or other groups to complete projects, studies, and risk assessments.</li><li>• 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.</li><li>• Evaluates and advises on organization, methods, and procedures.</li><li>• Analyzes management information requirements.</li><li>• Develops, analyzes, and evaluates new or modified program and management policies, regulations, goals, or objectives.</li><li>• Develops procedures and systems for assessing the effectiveness of programs and management processes.</li></ul>	
<b>Factor Levels</b>	
<p>FACTOR 1 KNOWLEDGE REQUIRED Level 1–8 1550 points</p> <ul style="list-style-type: none"><li>• 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.</li><li>• Knowledge of a comprehensive range of administrative laws, policies, regulations, and precedents applicable to the administration of one or more programs.</li><li>• 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.</li><li>• Knowledge of relationships with other programs and key administrative support functions within the program or other agencies.</li><li>• 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.</li></ul>	
<p>FACTOR 2 SUPERVISORY CONTROLS Level 2–5 650 points</p> <p>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</p>	

## Senior Risk Analyst

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 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

## Senior Risk Analyst

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 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”).

Category	Description
<b>Objectives</b>	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.
<b>Scope</b>	The Risk Committee shall monitor and discuss the financial exposures and activities of the [agency] for credit, market, liquidity, and operational risks.
<b>Functions</b>	The Risk Committee shall have the following functions: <ol style="list-style-type: none"><li>Monitor risk profiles and progress towards achieving policy goals for financial exposures and activities.</li><li>Receive updates on and discuss risk management matters and risk profiles of financial exposures and activities.</li><li>Advise program managers on the development and implementation of risk management guidelines, policies, and procedures with respect to financial exposures and activities.</li><li>Discuss agency-wide risk management practices.</li><li>Help develop risk management best practices.</li></ol>
<b>Organizational Structure</b>	The Risk Committee will be comprised of the following Members: <ol style="list-style-type: none"><li>Deputy head of [Agency], who will serve as Co-Chair</li><li>Chief Risk Officer, who will serve as Co-Chair</li><li>All Program Under Secretaries and Assistant Secretaries</li></ol>
<b>Meetings</b>	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. <ol style="list-style-type: none"><li>Minutes. The Office of Risk Management shall be responsible for preparing minutes of meetings.</li><li>Agenda. The Office of Risk Management shall provide to Members the meeting agenda at least 48 hours in advance of the meeting.</li><li>Attendance. Whenever appropriate, program managers and their supervisors will be invited to attend meetings of the Risk Committee at</li></ol>

	which their programs are being discussed or those where their expertise would be helpful to other programs.
<b>Staffing</b>	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.
<b>Amendments</b>	The Risk Committee will review this Charter at least annually and may amend it in its discretion.
<b>Effective Date</b>	This Charter is effective immediately.

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

Category	Description
<b>Purpose</b>	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).
<b>Authority</b>	<p>The Committee has authority to conduct or authorize reviews into any matters within its scope of responsibility. Specifically, it is empowered to:</p> <ul style="list-style-type: none"> <li>A. Retain independent counsel, advisors, or others to advise the Committee or assist in the conduct of its duties.</li> <li>B. Seek any information it requires from employees, all of whom are directed to cooperate with the Committee’s requests.</li> <li>C. Meet with the officers, external advisors, auditors, or outside counsel, as necessary.</li> <li>D. Discharge any other duties or responsibilities delegated to it.</li> </ul>
<b>Composition</b>	<p>The Committee will consist of at least three and no more than five members of the AGENCY leadership. Committee members should have:</p> <ul style="list-style-type: none"> <li>A. Expertise in risk governance and management, the risks the AGENCY faces, and methods for managing such risks.</li> <li>B. Expertise in business activities (including finance), processes and risks similar to the size and scope of the AGENCY.</li> <li>C. Expertise in risk committee functions.</li> <li>D. The time, energy, and willingness to serve as active contributors.</li> </ul>
<b>Meetings</b>	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>i.e.</i> , two members constitute a quorum if the Committee consists of three members; three members

	<p>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.</p> <p>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.</p>
<b>Committee Duties and Responsibilities</b>	<p>AGENCY management has the duties and responsibilities of risk assessment, monitoring, and management.</p> <p>The Committee has an independent oversight role and, in fulfilling that role, relies on reviews and reports provided by AGENCY's management.</p> <p>The Committee's duties and responsibilities shall include the following:</p> <ul style="list-style-type: none"> <li>A. Review and discuss with AGENCY management, and provide guidance on: <ul style="list-style-type: none"> <li>i. Risk governance structure and framework.</li> <li>ii. Risk appetite statement.</li> <li>iii. Policies for enterprise risk assessment, monitoring, and management of strategic, reputational, regulatory, operational, and financial risks.</li> <li>iv. Periodic reports on selected risk topics as the Committee deems appropriate.</li> <li>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.</li> </ul> </li> <li>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.</li> <li>C. Receive reports on the status of internal and external reviews and audits and reports from internal and external reviewers and auditors.</li> </ul> <p>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.</p>
<b>Management Responsibilities</b>	<p>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.</p>

### *c. Risk Committee Informal Charter (Example)*

This group will identify, track, and manage 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)*

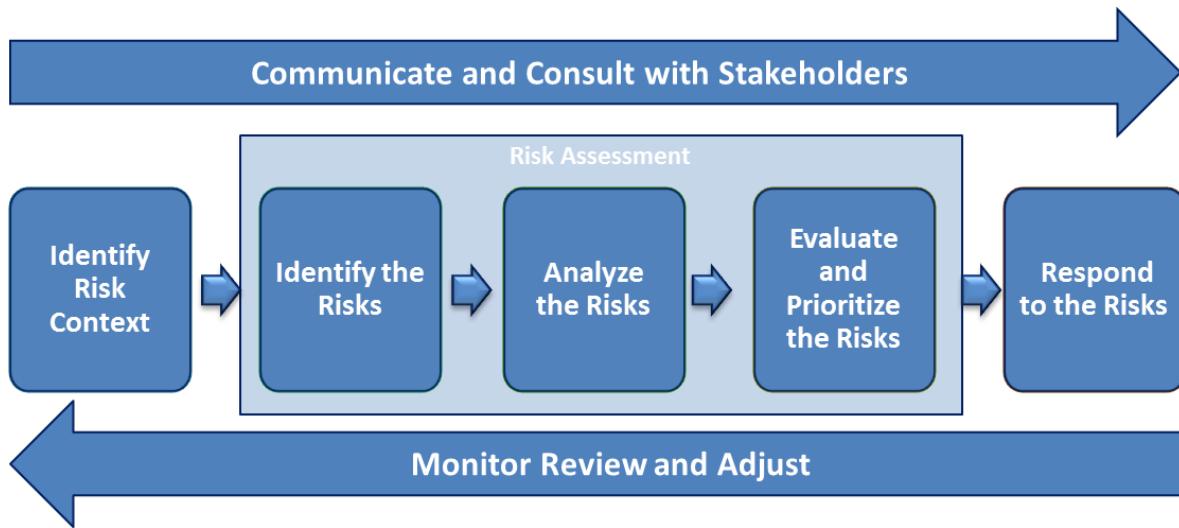
## Vision for Office of Risk Management

---

<u>What It Is</u>	<u>What It Is Not</u>
- 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: <ol style="list-style-type: none"><li>a) Risks are “locally” identified and owned</li><li>b) Risk measurement, mitigation, and monitoring tools are effectively deployed</li></ol>	- A substitute for risk ownership and management at the program level
- A leader in: <ol style="list-style-type: none"><li>a) Ensuring consistent identification of <i>individual</i> and <i>collective</i> program risks</li><li>b) Guiding the setting of risk appetites; identifying when Agency is at-risk of exceeding them</li></ol>	- “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. Enterprise Risk Management 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 a consistent risk management approach. The main elements of the [AGENCY] risk management process are depicted below.



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 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 by making 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. 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, avoid, pursue, reduce, transfer, or share 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 and Prioritization
  - Participants: ORM staff; office and 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 manage the risk.
4. Interim work: bureau and 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 and 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 and bureaus through Quarterly Performance Reviews, Strategic Objective Annual Reviews, discussions at Risk Management Committee meetings, [other].

***General Timeline for Maturing the Enterprise Risk Management 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, 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.

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.

## C. Enterprise Risk Management Frameworks

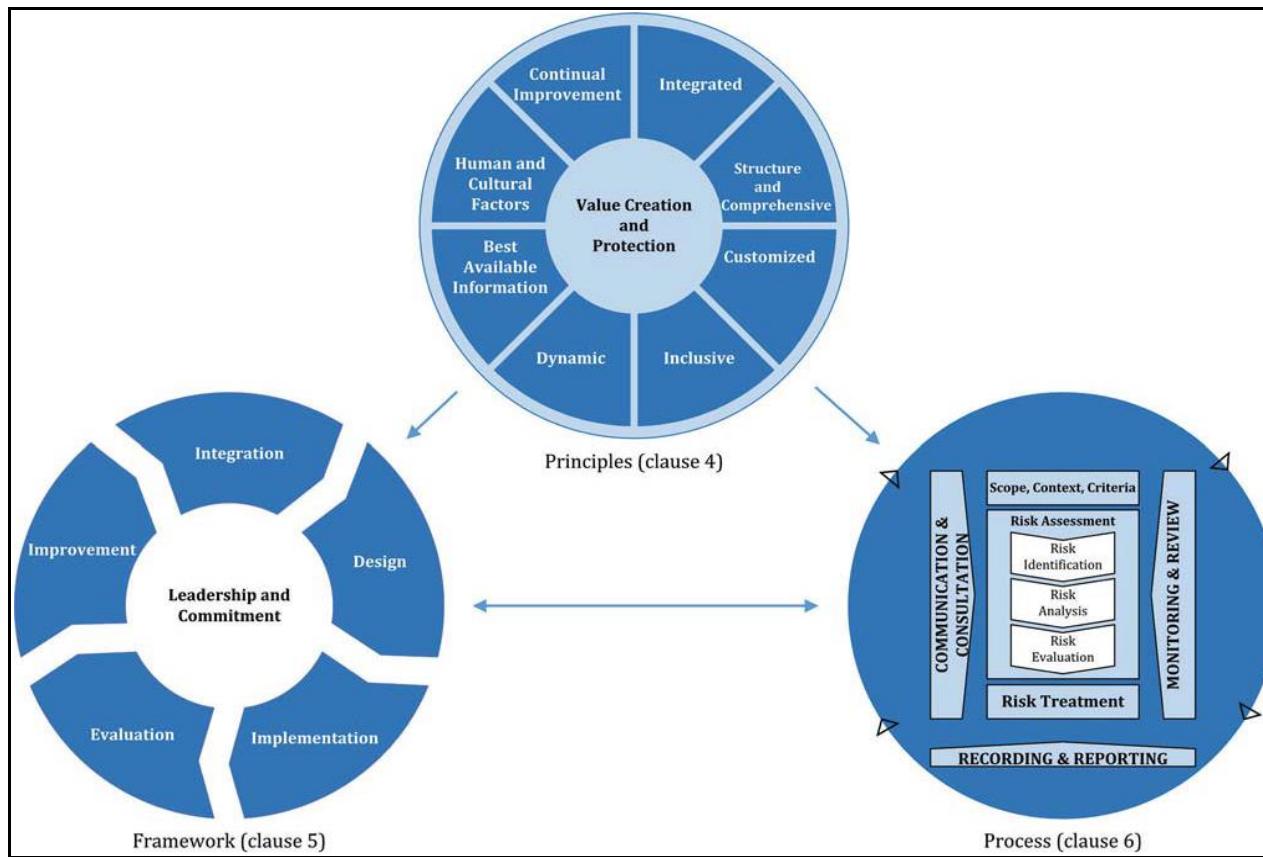
### a. COSO ERM Framework (Example)<sup>66</sup>

COSO 2017 updated the ERM framework to five interrelated components of risk management. Integration is emphasized to enhance performance by more closely linking strategy and business objectives to risk in order to provide a clear path to create, preserve, and realize value.



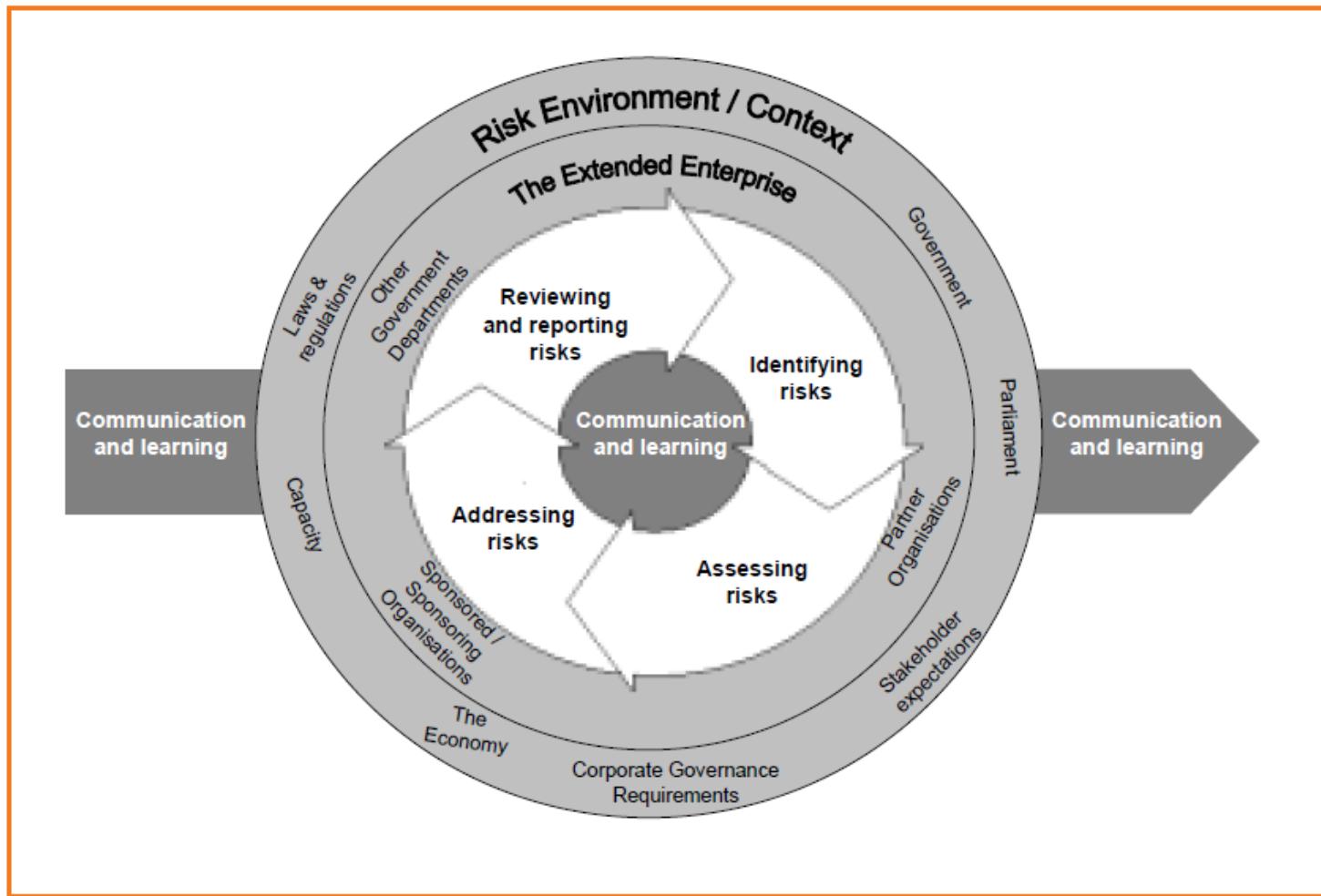
<sup>66</sup> Committee of Sponsoring Organizations of the Treadway Commission. *Enterprise Risk Management – Integrating with Strategy and Performance*, Executive Summary. 2017.  
[http://www.coso.org/documents/COSO\\_ERM\\_ExecutiveSummary.pdf](http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf)

**b. ISO 31000: Principles, Framework, and Process (Example)<sup>67</sup>**



<sup>67</sup> Risk management – Guidelines, International Organization for Standardization (ISO) 31000:2018. <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en>

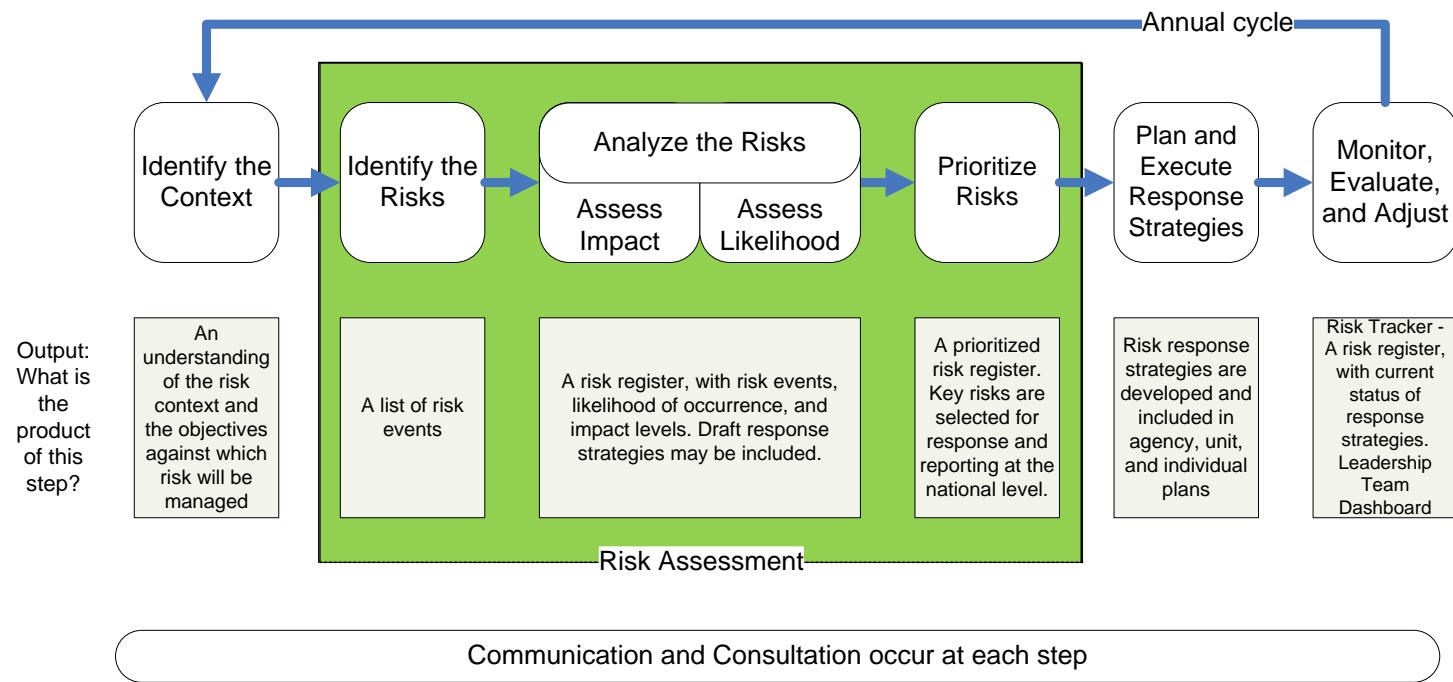
c. UK Orange Book Enterprise Risk Management Framework (Example)<sup>68</sup>



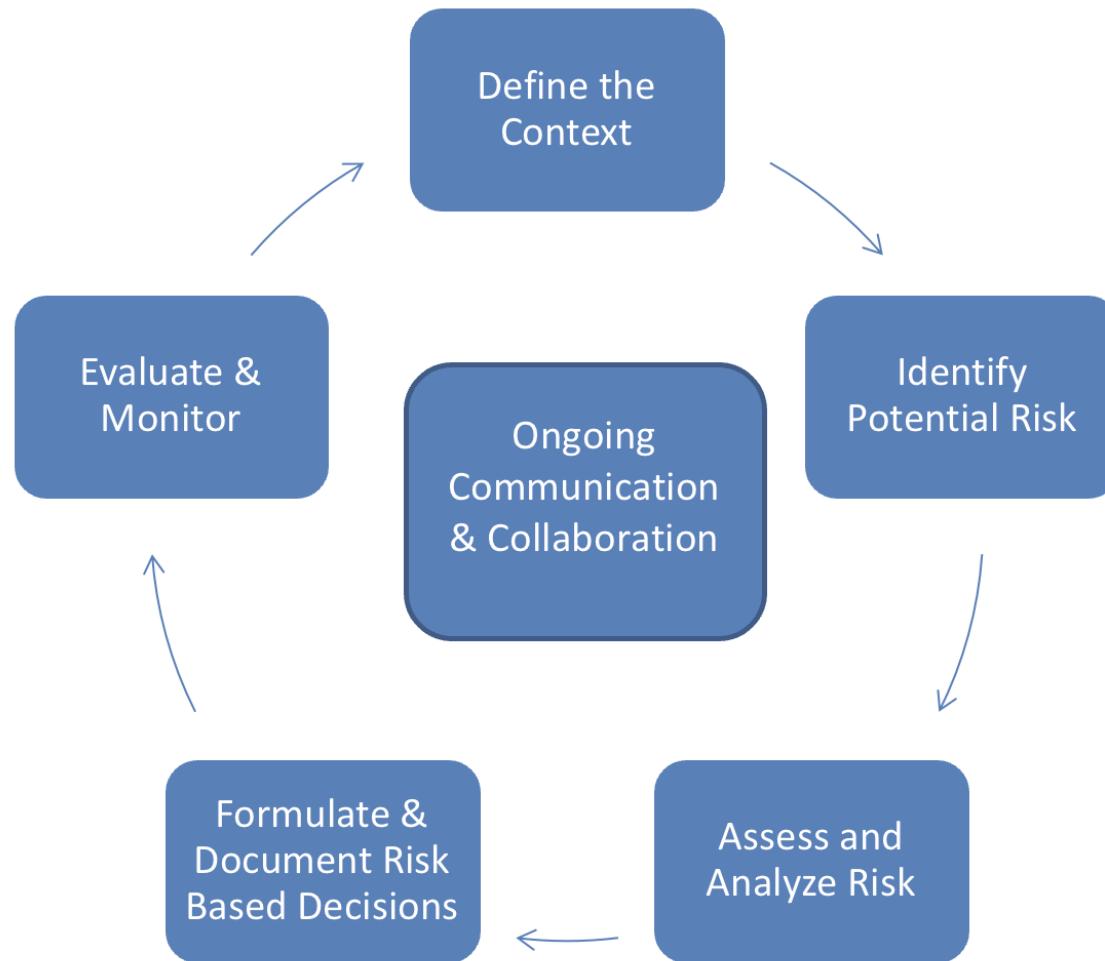
<sup>68</sup> UK Treasury. The Orange Book, Management of Risk – Principles and Concepts. 2004.

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/220647/orange\\_book.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf)

**d. Alternative Framework (Example)**



*e. Alternative Framework (Example)*



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

## D. Maturity Models

The maturity models shown in this appendix are intended to serve as benchmarking and management self-assessment tools that federal agencies and departments can use to build their ERM capabilities and communicate throughout the organization. These models may be used to continually self-assess the maturity of a federal ERM program and its supporting framework. The intent of the models is to provide criteria which can help an organization move forward over time, ultimately embedding ERM practices into daily business operations and strategic decision-making. Such an assessment is voluntary, and the models presented should not be used to prescribe how a federal enterprise implements ERM, as there is no one-size-fits-all approach.

*As mentioned earlier in the Playbook, risk management is everyone's responsibility, and it is important to foster an open environment that enables objective discussions about risks across the enterprise. As a result, these examples of maturity models:*

- Do not prescribe how to perform ERM.
- Provide a tool for the enterprise to continually self-assess its ERM program maturity, including related processes, governance, and value to the enterprise.
- Enable enterprise flexibility in implementing its ERM program to provide a balanced, portfolio view.
- Allows for information to flow both vertically and horizontally across the enterprise.
- Ensure that the enterprise is working from the same risk framework with a shared understanding of what the risks are (standardization/common language).
- Assist with senior management buy-in for continuous momentum, as well as strategic and resource prioritization and decision-making.
- Facilitate an integrated, holistic consideration of risks and opportunities with the strategic priorities of the enterprise.
- Are scalable for use by small and large departments, agencies, and components alike.

These maturity models depict the evolution and maturation of a federal ERM program. If they decide to use a maturity model to assess their ERM capabilities, federal agencies are encouraged to tailor any model to best meet their enterprise and business needs and objectives. For example, a well-defined ERM program can be recognized at a middle level of any maturity model. It may reasonably take multiple years to advance from one level to the next. Agencies may decide that they are comfortable running their program at a certain level, and that is sufficient. It is also very important to understand that the maturity level does not always move forward. When an agency changes leadership, is charged with another mission, or other priorities arise, the maturity in one or more areas of the ERM program may regress. That is to be expected under certain conditions.

While these models can be used to help inform oversight and information planning and can focus associated efforts on building value versus compliance, none of these models is intended to be used as a compliance checklist or audit tool. Federal ERM maturity self-assessments should be a means for agencies to identify next steps in their ERM program maturity curve - and not a mandate or expectation.

### a. Federal ERM Maturity Model (Example)

This Federal ERM Maturity Model was developed by a working group of federal ERM practitioners and incorporates common elements from existing ERM models and federal programs. It also considers best practices, lessons learned, and operational experiences from current federal ERM programs.

The model was purposefully structured to allow agencies to “score” themselves at different levels to reflect potential varied levels in maturity progression and time considerations. Agencies may assess themselves as mature in several, but not all, categories and similarly may find that they move up and down this maturity model. Agencies may continue to use their own models or variations of them to reflect their organizational needs and priorities.

This maturity model has 5 categories and each category has 5 distinct levels. Level 1 represents the lowest maturity and level 5 represents the highest maturity. The categories are as follows:

- Program Attributes: Specific to the key factors an internal ERM program should have when benchmarking itself. Expectations for behaviors of individuals who are engaged in the ERM program.
- Key Practices: Practices expected to be in place across the organization in terms of how ERM is implemented.
- Risk Culture: Progression of maturity achieved. How much of a focus is risk within the organization and how embedded is it within the agency’s culture. Includes approach to risk response.
- Organizational Benefits: The value provided by ERM to the enterprise.
- Executive Engagement: Tone at the top. Level of overall support.

A scale (chevron) is also included that envisions the relationship of the ERM program with the rest of the entity (i.e., internal relationship).

Recognizing agencies should, according to OMB A-123, “develop a maturity model approach towards the application of the federal ERM framework.” OMB engaged five federal agencies to pilot this Federal ERM Maturity Model. The selected agencies will complete self-assessments and validations of this model. The fundamental purpose of this pilot is to further mature the model based on the operational suggestions from the participating agencies. OMB’s intent for this pilot is for federal agencies to assess the effectiveness and ability of the model to measure and advance their ERM maturity. By doing so, agencies will foster an open environment that enables objective discussions about risks.

It is again noted that the Federal ERM Maturity Model is intended to be an enterprise self-assessment tool to help the “enterprise” achieve its own goals.<sup>69</sup> While this model can help to inform oversight and information planning, and focus associated efforts on building value versus compliance, it is not intended to be prescribed as a compliance checklist or an audit tool.

---

<sup>69</sup> Specific areas of interest which may utilize distinctively varying terminology, such as those related to cybersecurity and FISMA, should proceed cautiously and deliberately when attempting to apply this model.

# Federal Enterprise Risk Management (ERM) Maturity Model V1.0 (1/2020)

	<b>PROGRAM ATTRIBUTES</b>	<b>KEY PRACTICES</b>	<b>RISK CULTURE</b>	<b>ORG. BENEFITS</b>	<b>EXEC. ENGAGEMENT</b>	
Valued Partner	<b>Level 5: Optimized Predictive</b>	<ul style="list-style-type: none"> <li>Provides platform for enterprise agility &amp; innovation</li> <li>Leverage opportunities for informed risk taking and strategic planning</li> <li>Leverage internal/external horizon scanning to identify emerging risks</li> <li>Continuous improvement methods used to prepare for future</li> <li>ERM program facilitates knowledge sharing</li> </ul>	<ul style="list-style-type: none"> <li>Integrated external data sources that enhance insight</li> <li>Risk modeling / scenarios applied</li> <li>Risk appetite and tolerance clearly understood with alerts in place when thresholds exceeded</li> <li>Recognized as best in class</li> </ul>	<ul style="list-style-type: none"> <li>Risk response is anticipatory</li> <li>Stakeholders believe that risk management is everyone's job and there is an open environment that fosters objective discussions about risk across the enterprise</li> <li>Oversight entities are valued partners: Proactively engages and shares risk information with oversight entities. Regularly requests and integrates risk intelligence provided by oversight entities.</li> </ul>	<ul style="list-style-type: none"> <li>Resilient and agile enterprise built to pivot &amp; respond to opportunity &amp; change</li> <li>Extended enterprise embedded in strategic planning &amp; decision-making</li> <li>Transformational value to mission</li> </ul>	<ul style="list-style-type: none"> <li>Risk sensing discussions embedded in strategic planning and resource allocation</li> <li>External and internal executive champions align mission delivery to strategic objectives</li> <li>Engaging in sustained open dialogue</li> </ul>
Collaborative	<b>Level 4: Institutionalized Instilled</b>	<ul style="list-style-type: none"> <li>Identify opportunities for informed risk taking</li> <li>Coordinated risk mgmt. activities across identified segments</li> <li>Identify and document enterprise risk / reward trade off</li> <li>Enterprise governance considers risk during strategic goal setting and resource allocation</li> </ul>	<ul style="list-style-type: none"> <li>Instilled ERM discipline</li> <li>Fully standardized ERM processes integrated with tools and data</li> <li>Enterprise risk measured quantitatively/ qualitatively with interdependencies identified</li> <li>Define risk appetite and tolerances</li> </ul>	<ul style="list-style-type: none"> <li>Risk response is proactive and predictable</li> <li>Processes are monitored and reviewed for continuous improvement</li> <li>Open and inclusive environment and staff are encouraged to discuss risks internally</li> <li>Highly collaborative engagement with oversight entities: Actively engages and regularly shares risk information with oversight entities. Requests/seeks additional risk intelligence from oversight entities</li> </ul>	<ul style="list-style-type: none"> <li>Preventing issues and creating value</li> <li>Readily adaptable to mission / organizational change (external)</li> <li>Informed risk taking aligned with enterprise strategy</li> <li>High perceived value to mission</li> </ul>	<ul style="list-style-type: none"> <li>Executive ownership at enterprise level</li> <li>Risk discussions considered in strategic planning and resource allocation</li> <li>Decision making based on risk reward and trade-off issues</li> <li>Engaging in ERM open dialogue</li> </ul>
Cooperative	<b>Level 3: Defined Coordinated</b>	<ul style="list-style-type: none"> <li>Formally established roles and responsibilities</li> <li>Formal enterprise governance exists</li> <li>Some knowledge sharing across risk functions</li> </ul>	<ul style="list-style-type: none"> <li>Standardized ERM program and practices are documented</li> <li>ERM processes evolving but not fully integrated</li> <li>Enterprise risk measured/managed primarily qualitatively</li> <li>Enterprise risk information is routinely and consistently monitored and reported to support prioritization</li> <li>Introduction of risk appetite</li> </ul>	<ul style="list-style-type: none"> <li>Risk responses are focused on prevention</li> <li>Action plans implemented in response to high priority risks</li> <li>Collaborative engagement with oversight entities: Engages and shares risk information with oversight entities. Receptive to risk intelligence provided by oversight entities.</li> </ul>	<ul style="list-style-type: none"> <li>Moderate perceived value to mission</li> <li>Informs priorities for risk based decision making</li> </ul>	<ul style="list-style-type: none"> <li>Strategically reviewing top enterprise risk</li> <li>Actively promoting an open risk dialogue</li> <li>Familiarity with and initial training in ERM</li> </ul>
Developing	<b>Level 2: Fragmented Early Stages</b>	<ul style="list-style-type: none"> <li>Some enterprise governance</li> <li>Some ERM responsibilities built into existing roles</li> <li>Tactical</li> <li>Agency enterprise goals or objectives considered</li> </ul>	<ul style="list-style-type: none"> <li>Emerging enterprise risk management discipline</li> <li>Risks managed in silos (localized experiences/processes)</li> <li>Disparate monitoring / reporting</li> <li>Inconsistent risk definitions</li> </ul>	<ul style="list-style-type: none"> <li>Risk responses are functional, reactive problem solving</li> <li>Risk management for short term benefits</li> <li>Minimally predictive</li> <li>Cooperative engagement with oversight entities: Provides information and data to oversight entities (engagement-driven). Considers risk intelligence provided by oversight entities.</li> </ul>	<ul style="list-style-type: none"> <li>Independent risk activities</li> <li>Low perceived value to mission</li> <li>Compliance driven</li> </ul>	<ul style="list-style-type: none"> <li>Some management involvement when risk issues are reported</li> <li>Limited understanding of ERM and risk awareness</li> </ul>
Initial	<b>Level 1: Initial Ad-hoc</b>	<ul style="list-style-type: none"> <li>No formal cross-cutting ERM governance</li> <li>Decentralized roles / responsibilities</li> <li>Isolated risk management processes</li> <li>Transactional</li> </ul>	<ul style="list-style-type: none"> <li>Intermittent</li> <li>Few activities defined</li> <li>Quick-fix risk management</li> </ul>	<ul style="list-style-type: none"> <li>Risk responses are reactive</li> <li>Backward looking</li> <li>Unpredictable</li> <li>Minimal capacity to respond efficiently and effectively</li> <li>Cooperative engagement with oversight entities: Provides information and data to oversight entities (compliance-driven) Considers risk intelligence provided by oversight entities.</li> </ul>	<ul style="list-style-type: none"> <li>Unaware of the value of ERM</li> <li>Organization is not defined</li> </ul>	<ul style="list-style-type: none"> <li>Ad-hoc</li> <li>Haphazard feedback</li> <li>Informal (impromptu) input</li> </ul>

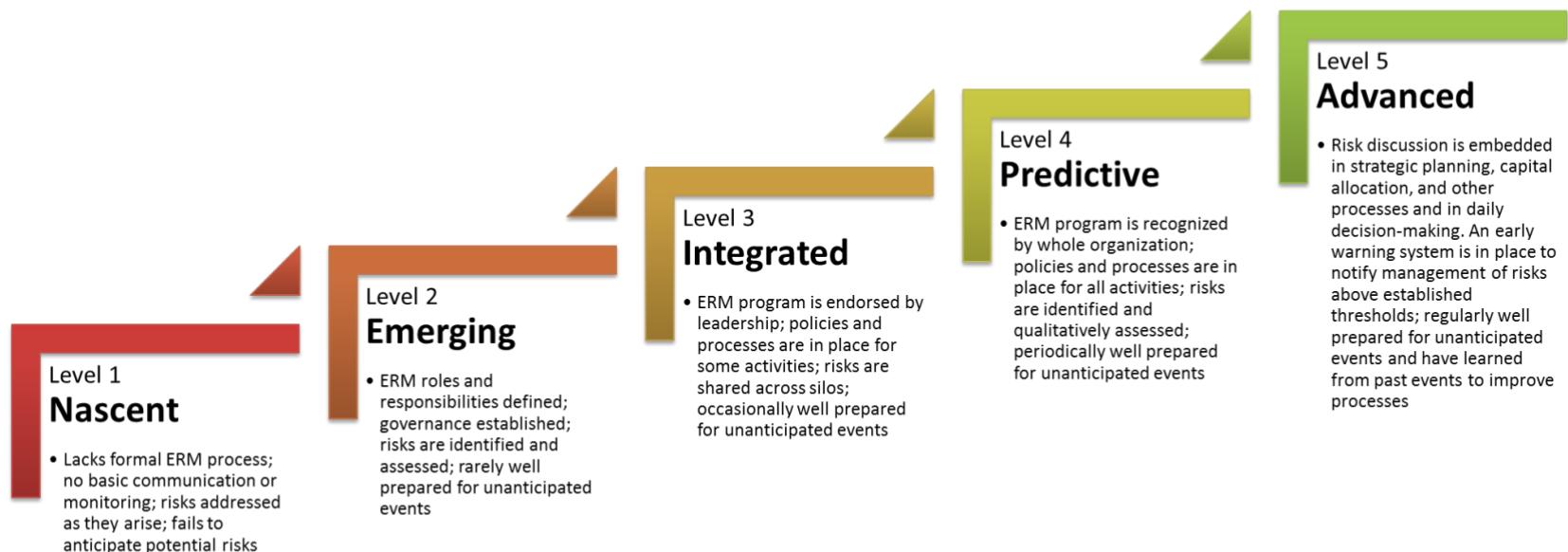
The material in this document should not be construed as audit guidance.

## b. Agency ERM Maturity Model (Example)

Enterprise Risk Management (ERM) Maturity Model Vers. 1.0 (Adapted from Federal ERM Model)						For illustration purposes only	
PROGRAM ATTRIBUTES	Level 1: Initial/Ad-hoc	Level 2: Fragmented/Early Stages	Level 3: Defined/Coordinated	Level 4: Institutionalized/Instilled	Level 5: Optimized/Predictive	Maturity Level	Supporting Comments
	No formal ERM governance exists	Informal ERM governance exists	Formal ERM governance exists	Embedded ERM governance exists	Effective ERM governance exists	5	Institutionalized/Instilled
	No centralized risk management roles/responsibilities	Some centralization of ERM responsibilities built into existing roles or siloed in various LOBs	Generally centralized ERM roles and responsibilities	Centralized and institutionalized ERM roles and responsibilities	Fully centralized ERM roles and responsibilities with CRO reporting directly to the top executive	4	
	ERM program does not facilitate knowledge sharing or leverage opportunities for informed risk taking	ERM program facilitates some knowledge sharing and opportunities for informed risk taking	ERM program generally facilitates knowledge sharing and opportunities for informed risk taking	Advanced ERM program that facilitates knowledge sharing and opportunities for informed risk taking	ERM program fully facilitates knowledge sharing and leverages opportunities for informed risk taking	3	
	Ineffective ERM framework and processes exist	Developing ERM framework and processes	Standardized ERM framework and processes exist with periodic monitoring for framework improvements	Managed ERM framework and processes exist and are regularly monitored and reviewed for improvements	Optimal ERM framework and processes exist and are proactively monitored and reviewed to prepare for the future	5	
						4.25	
KEY PRACTICES	Ad hoc enterprise risk management	Early stages of enterprise risk management	Coordinated ERM program and practices	Instilled ERM program and practices integrated with internal tools and data	Predictive ERM program which leverages external data sources that enhance insight and internal/external horizon scanning to identify emerging risks	3	Institutionalized/Instilled
	Initial activities defined	Emerging enterprise risk management discipline	Defined ERM processes yet not fully integrated	Instilled ERM discipline	Optimal ERM discipline, recognized as best in class	3	
	Reactive monitoring and reporting exists	Informal monitoring and reporting exists	Formal monitoring and reporting exist to support risk prioritization	Embedded monitoring and reporting exist and considers forward-looking/emerging risk areas to support risk prioritization and decision-making	Effective and efficient monitoring and reporting exist to support forward-looking risk taking, aligned with risk appetite, strategy and budget	4	
	No enterprise risks are measured or managed	Some enterprise risks are measured and managed	Enterprise risks are routinely measured/managed, primarily qualitatively	Majority of enterprise risks are measured quantitatively and qualitatively, with interdependencies identified and effectively managed	Enterprise risks are fully measured and managed (e.g., through risk modeling/scenarios)	4	
	No risk appetite in place	Fragmented risk appetite-in-place	Defined risk appetite in place	Institutionalized risk appetite and tolerances in place	Optimal risk appetite and tolerances established, clearly understood with alerts in place when thresholds exceeded	3	
							3.4
RISK CULTURE	Risk responses are reactive	Risk responses are developing	Risk responses are tactical, supported by action plans implemented in response to high priority risks, and focused on prevention	Risk response is strategic	Risk response is proactive	3	Defined/Coordinated
	Workforce has no understanding of ERM and risk concepts	Workforce has some understanding of ERM and risk concepts	Workforce generally understands ERM and risk concepts	Workforce understands ERM and risk concepts and is encouraged to discuss risk in an open and inclusive environment	Workforce fully understands and embraces ERM and risk concepts and believes that risk management is everyone's job. There is an open environment that fosters objective discussions about risk across the enterprise	3	
							3
							Defined/Coordinated
ORG. BENEFITS	Unaware of ERM value to mission	Low perceived value to mission	Moderate perceived value to the mission	High perceived value to mission such as preventing issues and creating value	Transformational value to mission	4	Defined/Coordinated
	No perceived benefit	Some benefit, compliance driven	Generally beneficial, informs priorities for risk-based decision-making	Consistently informed risk taking aligned with enterprise strategy (e.g., by identifying and documenting enterprise risk/rewards trade off)	Fully beneficial; proactively informs risk taking, as well as; provides platform for enterprise agility and innovation	3	
	Backward-looking and does not respond to opportunity and change	Slow to adapt to change	Readily adapts to change	Agile and resilient; adaptable to change	Anticipates change; forward-looking	3	
							3.33
EXEC. ENGAGEMENT	Negligible executive engagement	Fragmented executive engagement	Formal executive engagement	High executive engagement	Optimal executive engagement	5	Institutionalized/Instilled
	Ad-hoc risk discussions/dialogue at the executive level	Some routine risk discussions/ dialogue at the executive level	Routine risk discussions/dialogue at the executive level	Managed and active risk discussions/dialogue at the executive level that consider strategic planning, resource allocation, and decision-making based on risk reward and trade-off issues	Integrated risk discussions/ dialogue that embeds risk sensing into strategic planning, resource allocation, and decision-making based on risk reward and trade-off issues	3	
	No understanding of ERM and minimal risk awareness	Emerging understanding of ERM and risk awareness	General understanding and awareness of ERM and risks, initial training in ERM	Advanced understanding and awareness of ERM and risk. Executive ownership at enterprise level	Optimal understanding and awareness of ERM and risk	4	
							4.00
	Overall Score and Level of Maturity						3.60
							Defined/Coordinated

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

### *c. Five Step Maturity Model (Example)*



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

*d. Maturity Across Eleven Areas (Example)*

Maturity Sub-Factors	Maturity Levels				
	1 Nascent	2 Emerging	3 Integrated	4 Predictive	5 Advanced
<b>CULTURE</b>					
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
<b>PROCESS - ANALYTICAL</b>					
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
<b>PROCESS - ORGANIZATIONAL</b>					
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

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

Maturity Sub-Factors	Maturity Levels				
	1 Nascent	2 Emerging	3 Integrated	4 Predictive	5 Advanced
<b>IMPLEMENTATION</b>					
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 all processes, and select processes leverage [AGENCY] enterprise data sources	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
<b>OUTCOME</b>					
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

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

### *e. 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.

## E. Risk Assessment

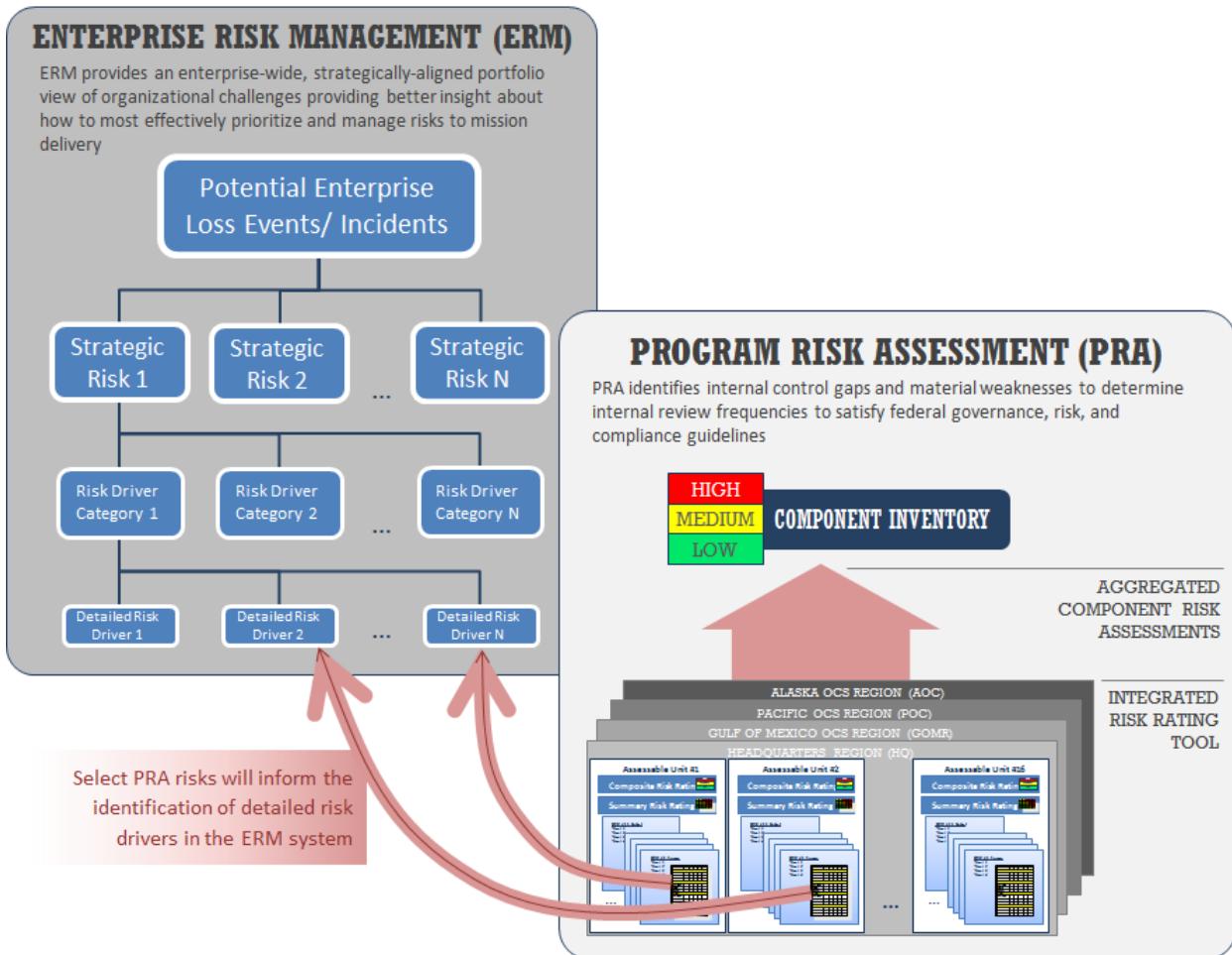
### 1. Establishing Context

#### a. Defining Context (Example)

Key Steps in Defining Context When Applying Risk Management Principles	
<b>Risk Tolerance and Risk Appetite</b>	Risk management efforts often involve tradeoffs between positive and less positive or 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.
<b>Scope &amp; Criticality of the Decision</b>	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.
<b>Establish Goals &amp; Objectives</b>	Ensure 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.
<b>Decision Timeframe</b>	Consider the timeframe in which a decision must be made, socialized, and executed, including time available for conducting formal analysis and decision review.
<b>Resources and Risk Management Capabilities</b>	Identify the staffing, budget, skill sets and 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.
<b>Availability and Quality of Information</b>	Consider the availability and quality of information that exists within the agency or 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.
<b>Decision Makers and Stakeholders</b>	Organizational leaders must be engaged at the beginning of a risk management and 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.
<b>Policies and Standards</b>	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 manage risk.

## 2. Risk assessments and the Enterprise Risk Management Process

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



## F. Risk Profile

### 1. Key Questions to Help Develop a Risk Profile

Step	Questions
<b>1. Communication and Consultation</b>	<ul style="list-style-type: none"><li>• Who needs to be involved?</li><li>• How will we communicate and consult with them?</li></ul>
<b>2. Identify Risk Context</b>	<ul style="list-style-type: none"><li>• What are your objectives?</li><li>• What are the things to consider when we assess the risks of achieving our objectives?</li><li>• What criteria will we use to assess our risks?</li><li>• Who will do the assessment?</li></ul>
<b>3. Identify the Risks</b>	<ul style="list-style-type: none"><li>• What events could happen that would affect my program areas or objectives?</li><li>• What are the corresponding impacts?</li></ul>
<b>4. Analyze the Risks</b>	<ul style="list-style-type: none"><li>• What is the severity of this impact according to accepted agency criteria?</li><li>• What is the likelihood this risk event will occur?</li></ul>
<b>5. Prioritize the Risks</b>	<ul style="list-style-type: none"><li>• What are the impact level and likelihood of your risks?</li><li>• How do the risks compare, such as on heat-map?</li><li>• Which risks does leadership consider the “top risks?”</li><li>• Which risks will require a response?</li></ul>
<b>6. Identify and Prioritize Risk Responses</b>	<ul style="list-style-type: none"><li>• What actions will we take to accept, avoid, pursue, reduce, transfer (or share) our risks?</li><li>• What actions are important to take now?</li><li>• Are there ongoing actions to continue?</li><li>• Who is accountable, when will they start, and when will it be done?</li></ul>
<b>7. Monitor, Evaluate, and Adjust</b>	<ul style="list-style-type: none"><li>• What is the status of our response actions?</li><li>• Are they completed, in progress, not started, or has the action been deferred?</li><li>• Did the action have the desired effect? What is the residual risk and how should we respond?</li></ul>

## 2. Templates

### a. Sample Risk Profile #1

RISK	Inherent assessment		RISK MITIGATION	Residual assessment		PROPOSED ACTION	OWNER	Proposed Action Category
	Impact	Likelihood		Impact	Likelihood			
<b>STRATEGIC OBJECTIVE – Improve program outcomes</b>								
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
<b>OPERATIONS OBJECTIVE – Manage This Risk of Fraud in Federal Operations</b>								
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	Risk Description	Strategy	Milestones/ Status	Progress Made	Likelihood (1-5)	Impact (1-5)	Trend Year Over Year	Strategic Objective Affected

*d. Sample Risk Profile #4*

Top Risks - (OFFICE OR BUREAU HERE)			
Risk Short Name:			
Risk Description:		Risk Rating	
Departmental Strategic Objectives Affected:		Impact (1-5)	Likelihood (1-5)
		Trending	
↓      ↔			
Potential Impacts		Current Status / Progress Made	
Proposed Mitigations		Milestones	

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

e. Sample Risk Profile #5

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 (6)	Probable (4)	Critical (20)	1. Mitigation Strategy #1. 2. Mitigation Strategy #2. 3. Mitigation Strategy #3. 4. Mitigation Strategy #4.	Critical (6)	Possible (3)	High (16)
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 (8)
4	Risk D	Significant (3)	Possible (3)	Medium (8)	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)

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

*f. Sample Risk Profile #6*

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.

*g. Sample Risk Profile #7*

		Significant Operational Issues Dashboard					
		Risk Impact	DATE Likelihood of Occurrence	Risk Impact	DATE Likelihood of Occurrence	Trending	
<u>Current Risks</u>		<u>Strategies</u>	-	-	-	-	
A.	Sample Risk #1	<ul style="list-style-type: none"> <li>Strategy #1.</li> <li>Strategy #2.</li> <li>Strategy #3.</li> </ul>	3	2	3	2	Neutral
B.	Sample Risk #2	<ul style="list-style-type: none"> <li>Strategy #1.</li> <li>Strategy #2.</li> <li>Strategy #3.</li> </ul>	3	3	3	4	Negative
C.	Sample Risk #3	<ul style="list-style-type: none"> <li>Strategy #1.</li> <li>Strategy #2.</li> <li>Strategy #3.</li> </ul>	5	4	5	3	Positive
D.	Sample Risk #4	<ul style="list-style-type: none"> <li>Strategy #1.</li> <li>Strategy #2</li> <li>Strategy #3.</li> </ul>	2	3	2	3	Neutral
E.	Sample Risk #5	<ul style="list-style-type: none"> <li>Strategy #1.</li> <li>Strategy #2.</li> <li>Strategy #3.</li> </ul>	5	2	5	3	Negative
F.	Sample Risk #6	<ul style="list-style-type: none"> <li>Strategy #1.</li> <li>Strategy #2.</li> <li>Strategy #3.</li> </ul>	4	5	4	3	Positive

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

### *h. Sample Risk Profile #8*

#### Risk Profile - Executive Summary

Strategic Initiative	Risk ID	Risk Title	Mitigation Coverage	Risk Trend	Residual Risk Level
Protect Consumers	P.1	Appropriately tailoring regulatory activities based on risk	●	►	Low
Manage Resources	P.2	Human capital management	○	▲	Elevated
	P.3	Employee health and safety	○	▲	Medium
Manage Resources (Information Technology)	P.4	Major cyber-attack	●	►	Medium
	P.5	Modernizing IT infrastructure and applications	○	►	Elevated

**Mitigation Coverage**                                    **Risk Trend**  
 ● High ○ Medium ○ Low    ▲ Increasing ► Stable ▼ Decreasing

### 3. Risk Assessment Tools

#### a. Example #1

##### Likelihood Scale

Likelihood	Definition
<b>1 - Very Low</b>	Risk event <b>rarely</b> to occur or occurs less than once every 10 years.
<b>2 – Low</b>	Risk event <b>unlikely</b> to occur, or occurs less than once a year, but more than once every 10 years.
<b>3 – Medium</b>	Risk event <b>possible</b> to occur or occurs between 1–10 times a year.
<b>4 – High</b>	Risk event <b>highly likely</b> to occur or occurs between 11–50 times a year.
<b>5 – Very High</b>	Risk event <b>almost certain</b> to occur, <b>or</b> 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
Business Impact	Very Low	Very Low	1	2	3	4	5	
	Low	Low	2	4	6	8	10	
	Moderate	Moderate	3	6	9	12	15	
	High	High	4	8	12	16	20	
	Very High	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 manage 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	Red
Medium Priority	5 - 14	Yellow
Low Priority	1 - 4	Green

**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 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 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	<u>Severely understaffed or no experience:</u> It is unrealistic to expect the staff assigned not to need supplementation or augmentation before the end of the effort	<u>None:</u> There are no documented or relevant procedures	<u>None:</u> There are no documented or relevant guidance	<u>A lot of:</u> There are historical events that tie directly to the problem history	<u>Cutting Edge:</u> No one has addressed this type of work in this program area or objective before	<u>Almost Certain:</u> The program area or objective involves integration of multiple agencies, consultants and contractors	<u>Almost Certain:</u> Numerous outside agencies and the public have the opportunity and ability to voice concerns, influence or direct	<u>A lot of:</u> There is almost no oversight and a almost no ability to identify waste, fraud and abuse	<u>None:</u> There are no training or mentoring programs	<u>None:</u> Division office personnel have no visibility or no management control	<u>A lot of:</u> The Agency is using a broad range of consultant to address the program area or objective	
Likely	<u>Understaffed or no experience:</u> Staff assigned will be over utilized and likely incapable of completion of without immediate training.	<u>Some:</u> There are some documented procedures or tangentially related procedures	<u>Some:</u> There is some documented guidance or tangentially related guidance	<u>Some:</u> There have been some incidents of problems related to this program area or objective in this type of program	<u>Done in other transportation agencies:</u> This type of work has been done in other transportation agencies, but no experience at this agency	<u>Likely:</u> The program area or objective involves integration of multiple agencies	<u>Likely:</u> One or two outside agencies and the public have the opportunity and ability to voice concerns, influence or direct	<u>Some:</u> There is some oversight, but certain gaps in our ability to identify waste, fraud and abuse	<u>Limited:</u> There are training and/or mentoring programs, but no funding and/or leadership commitment	<u>Limited:</u> Division office personnel have visibility but no management control	<u>Some:</u> The Agency is sharing significant responsibilities with consultants related to this program area or objective	
Possible	<u>Understaffed or some experience:</u> Staff assigned will be over utilized and run the risk of being incapable of completion if additional responsibilities are assigned, or lack experience	<u>Out-of-date:</u> There are documented procedures, but they are out-of-date with existing laws and regulations.	<u>Out-to-date:</u> There are documented guidance, but they are out-of-date with existing laws and regulations.	<u>Possible:</u> There are rumors or organizational legend of problems related to this program area or objective in this type of program	<u>Some experience:</u> Some people have done this type of work in the past or have done related work	<u>Possible:</u> This program area or objective involves integration of Agency and one other outside agency	<u>Possible:</u> One or two outside agencies have the opportunity and ability to voice concerns, influence or direct	<u>Possible:</u> There is oversight, but possible gaps in our ability to identify waste, fraud and abuse	<u>Some:</u> There are training and/or mentoring programs, but they are not universally available	<u>Some:</u> Division office personnel have management control over some aspects of the program area or objective	<u>Limited:</u> The Agency is sharing limited responsibilities with consultants related to this program area or objective	
Unlikely	<u>Adequately staffed or competent:</u> Adequately staffed or competent	<u>Good and up-to-date:</u> Procedures are good and up to date.	<u>Good and up-to-date:</u> Guidance is good and up to date.	<u>None:</u> There have been no significant or ongoing problems.	<u>Old news:</u> It's what we do, routine	<u>Unlikely:</u> This program area or objective involves only Agency personnel	<u>Unlikely:</u> There is virtually no opportunity or ability for outside agencies to voice concerns related to this program area or objective	<u>None:</u> There is virtually total oversight and a high opportunity to identify waste, fraud and abuse	<u>A lot of:</u> There are training and mentoring programs, broadly available to personnel	<u>A lot of:</u> Division office personnel have active management control over most aspects of the program area or objective	<u>None:</u> The Agency has full responsibility for all aspects of this program area or objective	

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

## 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 by the US Supreme Court, thereby effectively eliminating it nationally. Complete inability to achieve any of the programs 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 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 re prioritization. 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 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 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 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 measurable impact to protected rights or intended benefits of individuals.	Some localized, short-term economic disruption

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

## 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 findings.				
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.				
Insignificant or Neutral	Minimal or no measurable operational impact. Can be managed with routine activities. Leads to immaterial audit findings.				
	<b>How to use this Tool:</b> 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.				

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

*c. Example #3*

		Likelihood					
		Rare (1)	Unlikely (3)	Possible (5)	Likely (7)	Certain (9)	
		Description	Risk event could possibly occur, but is unlikely at this time	Risk event could occur under specific conditions and some of those conditions are currently evidenced	Risk event is likely to occur in most circumstances	Risk event is expected to occur in most circumstances	Risk event is occurring now
Impact	Catastrophic (9)	Large unacceptable financial loss, severe budget variance. Very significant harm to reputation with substantial impact on effectiveness. Large and unacceptable operational impact, long-term business interruption. Modified audit opinion.	9	27	45	63	81
	Significant (7)	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.	7	21	35	49	63
	Moderate (5)	Significant financial loss and variance to budget. Moderate embarrassment impacting short-term effectiveness. Moderate operational impact, business not interrupted. Leads to reportable findings.	5	15	25	35	45
	Low (3)	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.	3	9	15	21	27
	Insignificant (1)	Minimal or no measurable operational impact. Can be managed with routine activities. Leads to immaterial audit findings.	1	3	5	7	9

*d. Example #4*

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

## 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 <u>Highest Severity</u> <ul style="list-style-type: none"> <li>Safe: Two or fewer deaths</li> <li>Clean: Spill of 20,000 bbls or less</li> </ul>	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 <u>Highest Severity</u> <ul style="list-style-type: none"> <li>Safe: 2 to 10 deaths</li> <li>Clean: Spill of 20,000 to 100,000 bbls</li> </ul>	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 <u>Highest Severity</u> <ul style="list-style-type: none"> <li>Safe: 10 to 100 deaths</li> <li>Clean: Spill of 100,000 to 500,000 bbls</li> </ul>	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 <u>Highest Severity</u> <ul style="list-style-type: none"> <li>Safe: 100 to 1,000 deaths</li> <li>Clean: 500,000 to 5 million bbls</li> </ul>	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 <u>Highest Severity</u> >5 million	Example: Completely unable to perform mission and requiring complete re-commissioning with new leadership and complete reorganization 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	

<b>Very High</b>	> 5 million bbls of crude oil released	> \$100 Billion		Completely unable to perform mission and requiring complete re-commissioning with new leadership and complete reorganization with new management systems. (Mission impacts exceeding the Deepwater Horizon impacts.)
<b>High</b>	>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.
<b>Medium</b>	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.
<b>Low</b>	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.
<b>Very Low</b>	<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.

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

## 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				
		Very Low	Low	Medium	High	Very High
LIKELIHOOD	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.

*e. Example #5*

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 into 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 of 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.

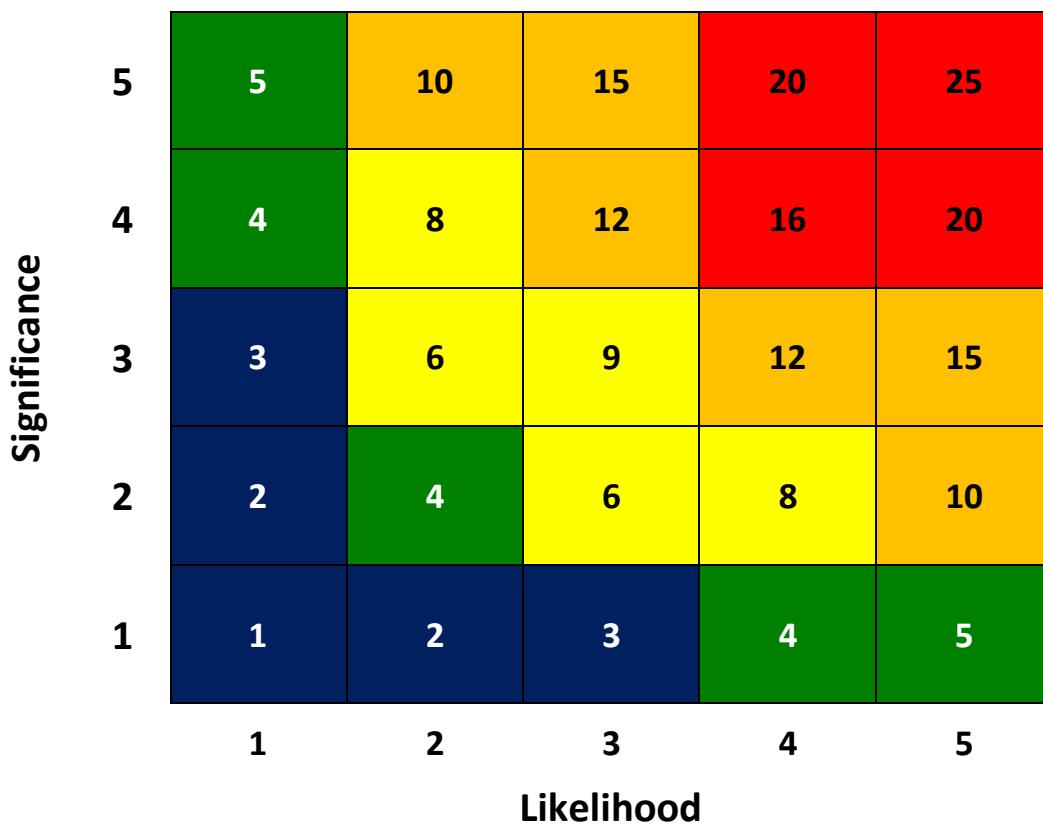
**Moderate (Rating-2)** – Risks that may have discernable impact on the business unit and/or area. Moderate risks can hamper the ability of a business unit or area to achieve one or more objectives, usually those of lesser significance. Occasionally they will rise to the level where they could actually 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 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 to 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 risk management strategy in place.	0 – 10	Key accountable parties monitor these risks and escalate issues if / when they arise. As 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 a strong risk management strategy 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. Risk management strategies are in place but may not be robust enough to prevent the risk from occurring. However, the risk management strategies in place would most likely lessen the chance of occurrence.	35 – 65	Reasonably certain that some level of risk management strategy exists. 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 certainty that the risk will occur. A risk that has more than a 50 percent chance of occurring. Effective risk management strategy is in place or are not functioning as intended.	65 – 90	RM works with key accountable parties on a regular basis to ensure risk management strategy exist.
5	Very Likely	A risk that is occurring or is certain to occur given the environment or factors involved. Risk management strategy is not in place or are not functioning as intended.	90 – 100	RM works aggressively with key accountable parties to ensure risk management strategy exist.



#### Aggregate Risk Scores<sup>70</sup>

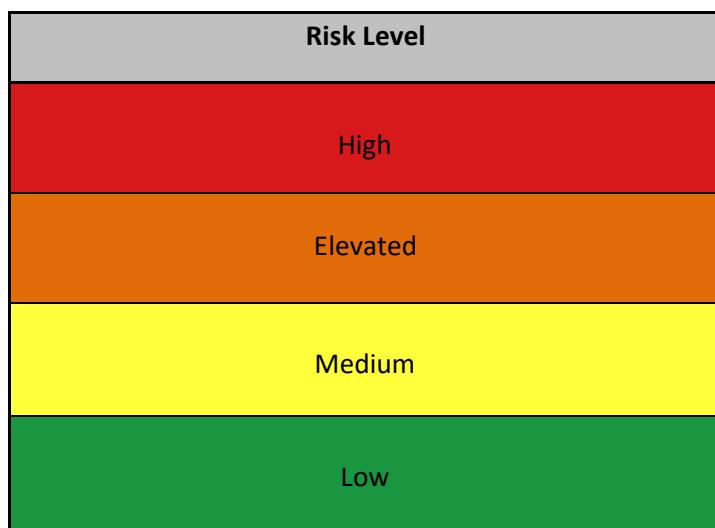
Critical (20-25)	-	
High (12-16)	-	
Medium (6-10)	-	
Moderate (4-5)	-	
Low (1-3)	-	

---

<sup>70</sup> Cumulative risk scores are calculated by multiplying the significance and likelihood ratings of a particular risk.

*f. Example #6*

Risk Rating Matrix				
Impact	Likelihood			
	Probable	Likely	Possible	Unlikely
	(100% - 76%)	(75% - 51%)	(50% - 26%)	(25% - 1%)
Critical				
Significant				
Moderate				
Low				



## G. Risk Reporting and Monitoring

### 1. Dashboards<sup>71</sup>

Portfolio Summary Dashboard					DATE													
Program Status				Bond Loan Payment Cycle		Portfolio Summary Characteristics												
Program Metrics		FY 20xx Cohort	FY 20xx Cohort	FY 20xx Cohort	Program Total	Portfolio Metrics												
Loan Authority (\$, millions)						Weighted Avg. Portfolio Duration: (modified)												
Applications						Interest Rate Spread (gross of fees)												
Funds Requested (\$, millions)						Collateral												
Funds Obligated (\$, millions)						Weighted Avg. Term-to-Maturity												
Loans						Weighted Avg. Interest Rate												
Advances																		
Status of Condition						Key Program Developments and Ongoing Risk												
<table border="1"> <tr> <td>Stable</td> <td>Watch List</td> <td>Special Asset</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> <tr> <td colspan="3">Watch List</td><td colspan="3" rowspan="5">Write bullets about key developments and changes in the portfolio and risk areas.</td></tr> </table>						Stable	Watch List	Special Asset				Watch List			Write bullets about key developments and changes in the portfolio and risk areas.			Write bullets about key developments and changes in the portfolio and risk areas.
Stable	Watch List	Special Asset																
Watch List			Write bullets about key developments and changes in the portfolio and risk areas.															
Insert Pie chart to show internal ratings for borrowers																		
Insert map with shading for exposure areas																		
Rating						Policy Metrics												
<table border="1"> <thead> <tr> <th>Ratings</th> <th>Participant ID</th> <th>Rating Weights*</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> </tr> </tbody> </table>						Ratings	Participant ID	Rating Weights*				Write or show how you are attaining your program's policy goals						
Ratings	Participant ID	Rating Weights*																

<sup>71</sup> Please see OMB Circular No. A-129 Appendix D for many examples of dashboards that include risk analysis.

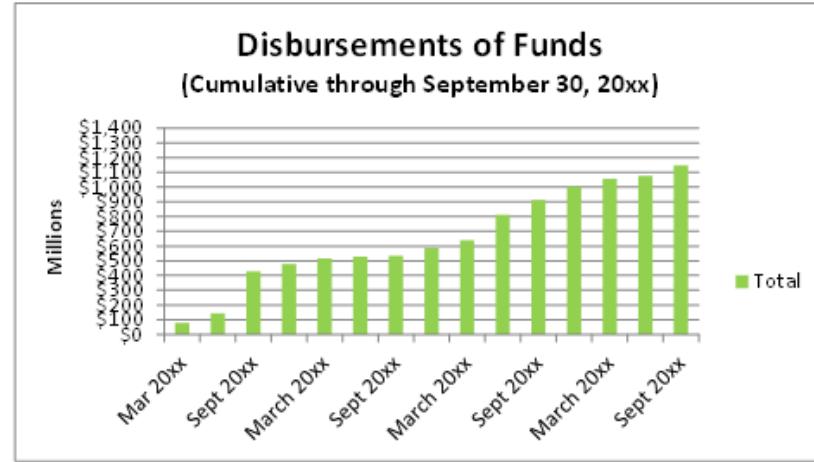
[https://www.whitehouse.gov/sites/default/files/omb/assets/a129/rev\\_2013/pdf/a-129.pdf](https://www.whitehouse.gov/sites/default/files/omb/assets/a129/rev_2013/pdf/a-129.pdf)

## Grant Program Dashboard As of DATE

Allocated and Deployed Funds		% of Total Allocated Funds
Allocated Funds	\$	
Total Funds Deployed	\$	
<i>Original Deployed</i>	\$	
<i>Recycled Funds Deployed</i>	\$	

Portfolio Summary			YOY Change
	12/31/20xx	12/31/20XX	
Total Private Financing (cumulative)	\$	\$	0%
AGENCY Dollars Expended (cumulative)	\$	\$	50%
Private Leverage (cumulative)			100%
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	

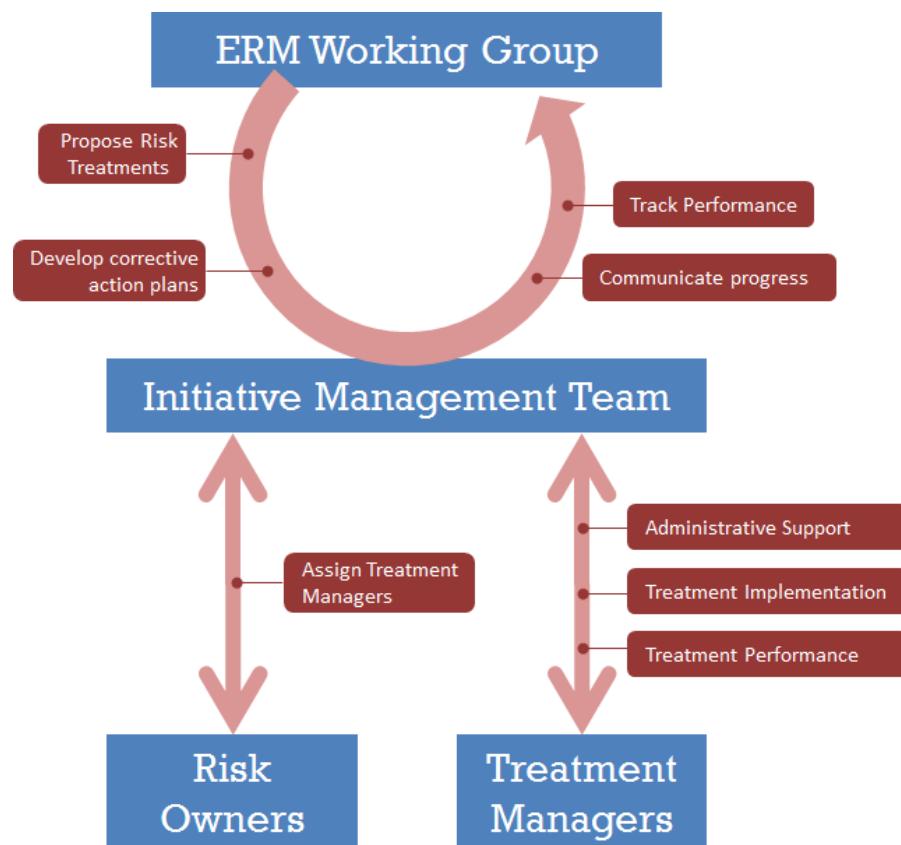


The material in this document should not be construed as audit guidance.

## 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
1				
2				
3				
4				
Contingency Plan:				Trigger:
Treatment Alternatives Considered				

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

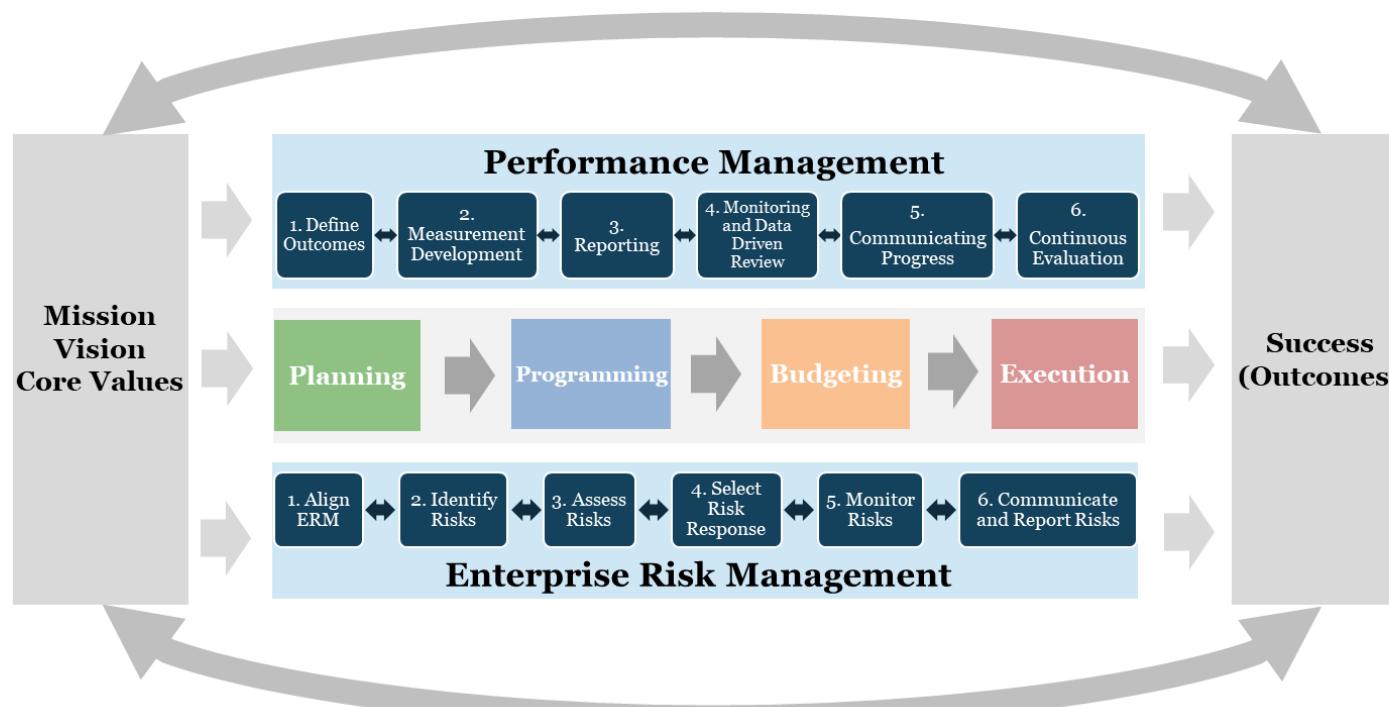
## H. Linking Risk and Performance

### Enterprise Risk Management

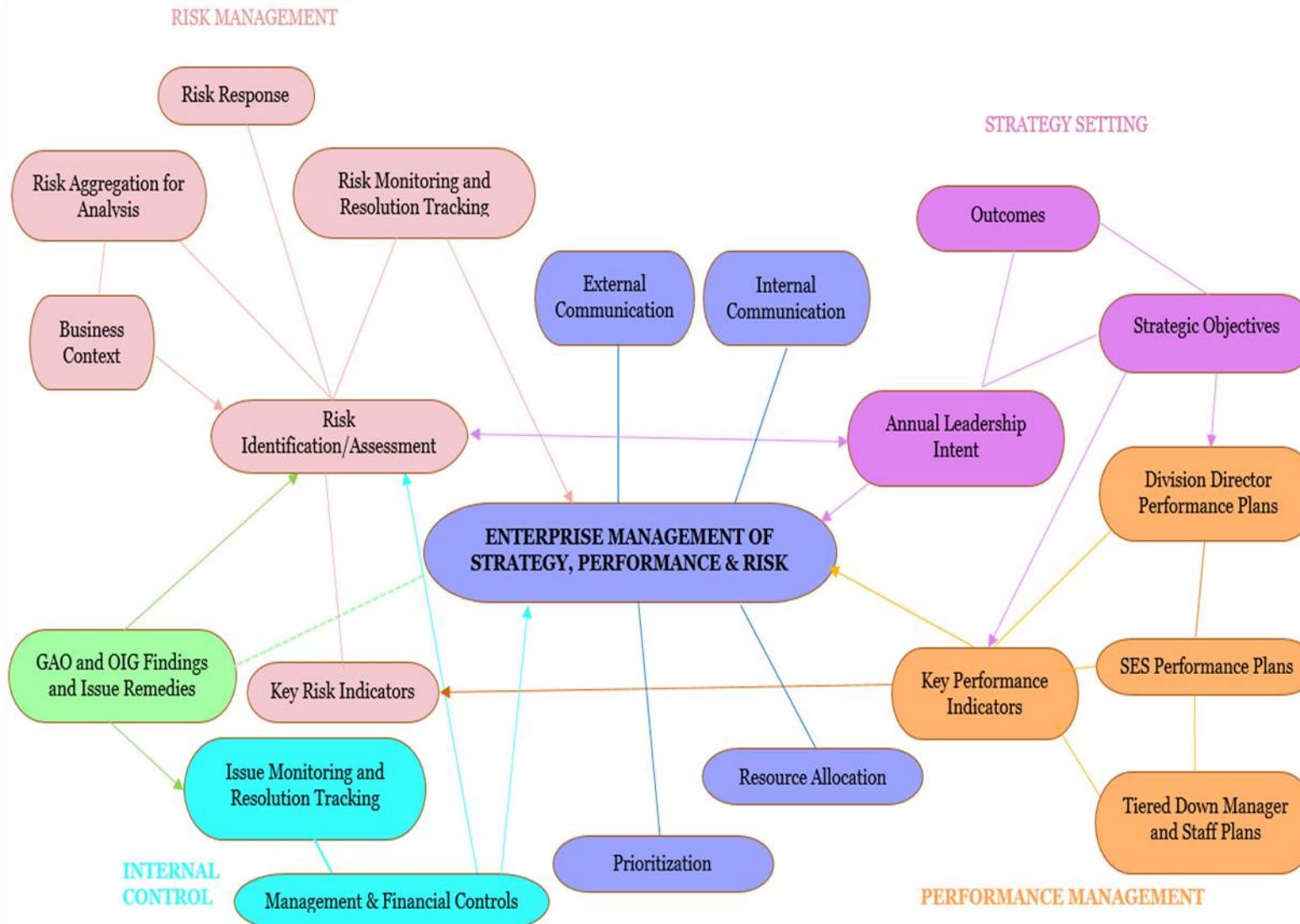
What prevents us from getting there?

Where are there opportunities to add value?

2



**ERM Program integrates Risk Management with Strategy Setting and Performance Management to enable risk-based decisions, risk-informed strategy setting, and effective risk and performance monitoring.**



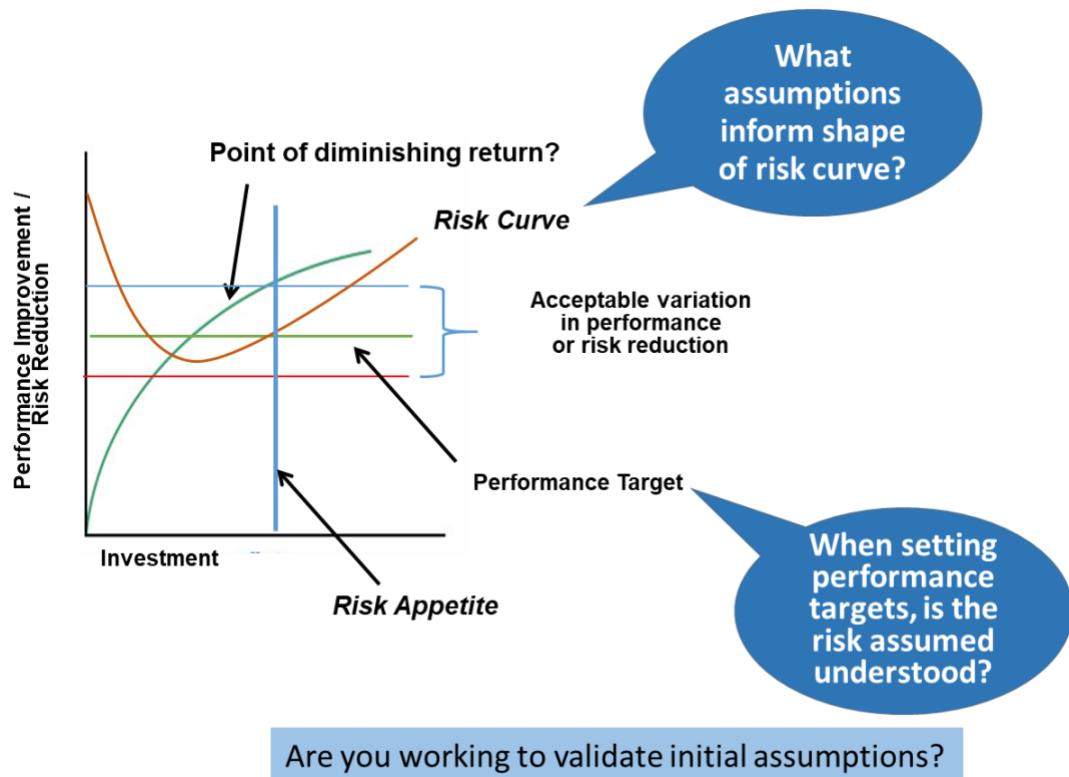
## I. Risk Appetite

### Key Performance, Risk Indicators and Risk Appetite

Key performance and risk indicators are similar in nature. Both address a range of expected performance that is based on risk appetite. Falling below expected performance for both key risk or performance indicators may signal the need to consider additional resources (time and/or money) or a reassessment of the risk appetite or risk response if this does not qualify for additional resources. On the other hand, consistent over performance may signal you have you may be overinvesting, and therefore may need to re-evaluate to see if the targets should be adjusted. “Tolerance” means there is an acceptable range or variation of performance or risk within a particular measure or indicator. Avoid the use of “go/no go” measures such as “achieve zero percent deficiencies” or “achieve 100 percent compliance” where possible.

While this graphic displays a single performance or risk indicator in isolation, in most organizations there are numerous indicators to be developed and tracked that provide a more holistic assessment of performance and risk across a program, functional portfolio, or organization/enterprise.

As with most programs, projects, or activities, we base initial performance/risk measurements using available information. Over time, seek to reduce uncertainty and reliance on assumptions through fact finding and data collection and analysis.



## J. Glossary

Term	Definition
<b>Acceptance</b>	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.
<b>Aggregate Risk</b>	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 designed to manage exposure to the specified risk.
<b>Application Controls</b>	Programmed procedures in application software, and related manual procedures, designed to help ensure the completeness and accuracy of information processing.
<b>Avoidance</b>	Risk response where action is taken to stop the operational process, or the part of the operational process causing the risk.
<b>Capital</b>	General term that refers to financial assets, the financial value of assets such as cash, or other financial resources available for use by an organization.
<b>Compliance Risk</b>	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.
<b>Computer Controls</b>	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.
<b>Control Activities</b>	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.
<b>Control Self-Assessment</b>	A process through which internal control effectiveness is examined and assessed. The objective is to provide reasonable assurance all business objectives will be met.
<b>Controls</b>	Policies or procedures that are part of a system of internal control.

Term	Definition
<b>Corporate Governance</b>	The set of processes, customs, policies, and regulations affecting the way an organization is directed, administered, or controlled.
<b>COSO</b>	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: <i>Internal Control—Integrated Framework</i> , which provides for establishing internal control systems and evaluating their effectiveness. In September 2004, COSO released <i>Enterprise Risk Management – Integrated Framework</i> , which provides guidance and standards for implementing ERM. COSO updated the 2004 publication to address the evolution of enterprise risk management and the need for organizations to improve their approach to managing risk to meet the demands of an evolving business environment. The updated document, now titled <i>Enterprise Risk Management – Integrating with Strategy and Performance</i> (COSO 2017). In 2013, COSO also issued <i>Internal Control – Integrated Framework</i> (COSO 2013).
<b>Cost/Benefit Analysis</b>	A technique designed to determine the feasibility of a project or plan by quantifying its costs and benefits.
<b>Credit Program Risk</b>	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.
<b>Cybersecurity</b>	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
<b>Cybersecurity Risk</b>	The exploitation of vulnerabilities by threat actors to compromise device or data confidentiality, integrity, or availability.
<b>Cyber Supply Chain Risk (C-SCRM)</b>	Potential for harm or compromise that arises as a result of cybersecurity risks from suppliers, their supply chains, and their products or services. Cyber supply chain risks include threat and vulnerabilities of the products and services traversing the supply chain as well as the threats and vulnerabilities to the supply chain.

Term	Definition
<b>Enterprise Risk Management (ERM)</b>	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.
<b>Entity</b>	An organization established for a particular purpose (e.g., a corporation, government body, academic institution, etc.) Synonyms include organization and enterprise.
<b>Event</b>	An incident or occurrence, from sources internal or external to an entity, that affects achievement of objectives.
<b>Financial Risk</b>	Risk that could result in a negative impact to the agency (waste or loss of funds/assets).
<b>Financial Risk Management</b>	The practice of creating value in an organization by using financial instruments or models to manage exposure to risk.
<b>Fraud</b>	Dishonesty in the form of an intentional deception or a willful misrepresentation of a material fact.
<b>General Controls</b>	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.
<b>Government Performance and Results Act Modernization Act (GPRAMA)</b>	Requires agencies define mission success through strategic planning and priority-goal setting, and regular management routines for assessing progress against organizational goals and objectives. Specifically, the Act requires agencies revise strategic plans every 4 years, and assess progress toward strategic objectives annually.
<b>Impact</b>	The effect of an event on strategic goals and objectives. Impact can be positive or negative related to the organization's objectives.
<b>Information and Communications Technology (ICT) Supply Chain Risk Management</b>	The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains.
<b>Information Security</b>	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Term	Definition
<b>Information Technology</b>	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
<b>Inherent Risk</b>	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.”
<b>Integrity</b>	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.
<b>Interest Rate Risk</b>	The risk associated with fluctuations in interest rates and the impact on investments, loans, or business activities.
<b>Internal Control</b>	A process, affected by an organization's management or other personnel, designed to provide reasonable assurance regarding the achievement of objectives.
<b>Internal Control Environment</b>	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.
<b>ISO</b>	<p>ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). ISO released two publications that are useful to ERM programs:</p> <ul style="list-style-type: none"> <li>• <i>Risk management – Guidelines</i> (ISO 31000:2018). This document is for people who create and protect value in organizations by managing risks, making decisions, setting, and achieving objectives and improving performance.</li> <li>• <i>Risk management – Risk assessment techniques</i> (IEC 31010:2019). This document provides guidance on the selection and application of various</li> </ul>

Term	Definition
	techniques that can be used to help improve the way uncertainty is taken into account and to help understand risk.
<b>IT Controls</b>	Refers to the broad category of information technology controls including computer, application, and general controls.
<b>Key Performance Indicator</b>	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.).
<b>Key Risk Indicator</b>	Key Risk Indicators (KRI's) relate to a specific risk and demonstrate a change in the likelihood or impact of the risk event occurring.
<b>Legal Risk</b>	Risk associated with legal or regulatory actions and an agency's capacity to consummate important transactions, enforce contractual agreements, or meet compliance and ethical requirements.
<b>Legislative Risk</b>	Risk that legislation could significantly alter the mission (funding, customer base, level of resources, services, and products) of the agency.
<b>Likelihood</b>	The probability that a given event will occur.
<b>Liquidity Risk</b>	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).
<b>Management Controls</b>	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.
<b>Management Fraud</b>	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.
<b>Manual Controls</b>	Refers to controls performed manually, not by computer or some other automated means.

Term	Definition
<b>Objective Setting</b>	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.
<b>Occupational Fraud</b>	The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets.
<b>Operational Risk</b>	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.
<b>Opportunity</b>	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.
<b>Political Risk</b>	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.
<b>Privacy Risk</b>	Operations that process personally identifiable information (PII) through the information lifecycle to meet mission or business needs of an organization or "authorized" PII processing and, as a side effect, cause individuals to experience some type of problem(s).
<b>Probability</b>	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 another numerical metric.
<b>Pursue</b>	Action is taken to increase the level of risk taken to optimize performance without exceeding acceptable risk tolerance.
<b>Reduction</b>	Risk response where action is taken to reduce the likelihood or impact of the risk.
<b>Regulatory Risk</b>	The risk of problems arising from new or existing regulations. Such problems may include: changes in laws or regulations having a 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.

Term	Definition
<b>Reporting Risk</b>	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.
<b>Reputational Risk</b>	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.
<b>Residual Risk</b>	The amount of risk left over after action has been taken to manage it, such as establishing internal controls.
<b>Review (Verification and Validation)</b>	The process by which assessment of risks is evaluated by senior management.
<b>Risk</b>	The effect of uncertainty on achievement of objectives. An effect is a deviation from the desired outcome, which may present positive or negative results.
<b>Risk Action Plan (RAP)</b>	A set of actions designed to accept, avoid, pursue, reduce, or share identified risks. The plan may include intended outcomes and timetables and any other follow-up work necessary.
<b>Risk Appetite</b>	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.
<b>Risk Assessment</b>	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 to manage risk.
<b>Risk Assessment Score</b>	A weighting of a potential outcome (positive/negative) multiplied by probability of its occurrence and used to prioritize choices.
<b>Risk Impact</b>	A measurement of the effect that could result from the occurrence of a particular identified risk.
<b>Risk Management</b>	A coordinated activity to direct and control challenges or threats to achieving an organization's goals and objectives.

Term	Definition
<b>Risk Mitigation</b>	Strategy for managing risk that seeks to reduce the significance and/or likelihood of a given risk.
<b>Risk Profile</b>	A prioritized inventory of an organization's most significant risks.
<b>Risk Response</b>	Management's strategy for managing (or responding to) a given risk. Risk response strategies include: accept, reduce, avoid, pursue or share (or transfer).
<b>Risk Strategy</b>	Synonymous with risk response. The strategy for managing (or responding to) a given risk. Risk response strategies include: accept, avoid, pursue, reduce, or share.
<b>Risk Tolerance</b>	The acceptable level of variance in performance relative to the achievement of objectives.
<b>Sharing</b>	Risk response where action is taken to transfer or share risks across the organization or with external parties, such as insuring against losses.
<b>Significance</b>	Magnitude or potential impact of a specified risk.
<b>Strategic Risk</b>	Risk that would prevent an area from accomplishing its objectives (i.e., meeting the mission).
<b>Supply Chain</b>	Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.
<b>Technology Risk</b>	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.
<b>Uncertainty</b>	The inability to know in advance the exact likelihood or impact of future events.
<b>Value at Risk (VaR)</b>	Measure of how the market value of an asset or 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.

## K. Special Chapter: Cyber – ERM Integration Use Cases

### Use Case (1)

In the Fall of 2019, one government agency’s ERM Council – equivalent to the Risk Management Council (RMC) described in OMB A-123 – accepted a recommendation from its CISO Council to add the Department CIO and CISO as voting members to the ERM Council.<sup>72</sup> The CIO and CISO membership to the ERM Council is instrumental because: (1) it enhances the two-way information sharing and coordination between the ERM and information security communities within the agency; (2) it allows this agency to have the CIO and CISO community perspectives heard on a consistent and constant basis on cybersecurity risks and opportunities for the agency; and (3) it provides the agency CISO community timely access to ERM Council discussions, allowing for a more collaborative Cyber/ERM environment for CISOs to engage with on Department-wide risks and opportunities. These actions support the ability of this agency to establish and document a process for coordination between cybersecurity risk management and ERM functions. Additionally, as part of this agency’s strategic plan, and in line with OMB Memorandum 19-03, ERM includes a focus on “expanding the ERM community by engaging all levels of the organization to promote risk awareness and risk management.”<sup>73</sup>

- Successful Cyber/ERM integration at this agency is exemplified through collaboration efforts across the High Value Asset (HVA) Program, the Cybersecurity Risk Management Branch, and the ERM function. These teams are working together to update the agency’s cybersecurity risk management strategy and advocate for the integration with the agency’s ERM activities. This partnership has proven to be beneficial because the HVA Program crosscuts with several other agency entities, which allows for information sharing, enterprise planning, and risk management efforts shared across all stakeholder groups.
- Another example of cyber-ERM integration efforts is bridging the gap between the agency’s CISO community and the Continuity of Operations (COOP) community. The agency HVA Program has facilitated working relationships between the CISO community and COOP teams. This has led to an improved ability to understand and recognize the relationship between HVAs and critical IT systems that support the agency’s Primary Mission Essential Functions (PMEFs) and associated division-level Mission Essential Functions (MEFs), paving the way for prioritization of risks and opportunities across the agency and its divisions.

Activities associated with the implementation of OMB A-123 and OMB M-19-03 requirements illustrate how this government agency has improved their ability to identify and understand the specific risk

---

<sup>72</sup> In many agencies, the CISO reports to the CIO, so the CIO has a seat on the ERM Council, not the CISO. The CISO briefs the Council as needed on specific FISMA, IT security, or cybersecurity topics. In this agency, both the CISO and the CIO have seats on the ERM Council.

<sup>73</sup> OMB Memorandum 19-03 “Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program”, December 2018. This memo requires federal agencies take a strategic, enterprise-wide view of cyber risk that unifies the effort to protect HVAs against evolving cyber threats by designating an integrated agency-level office, team, or other governance structure to enable the incorporation of HVA activities into broader agency planning activities for information system security and privacy management such as ERM, Capital Planning and Investment Control (CPIC), Contract Management, and Contingency Planning.

management and security needs of their most critical assets while gaining new insight into how those assets fit into the larger agency enterprise and ultimately the federal enterprise.<sup>74,75</sup>

### **Use Case (2)**

In at least two government agencies, the ERM Council established an audit committee (chaired by the DCIO and DCFO) to review financial, IT, and other non-financial audits in detail for discussion and escalation to the ERM Council using a common set of escalation criteria. In this way, the governance structure for ERM within the agencies was strengthened because the audit committee was given a delegated responsibility to assess trends, emerging risks, and impacts to the agency across multiple risk categories, including reputational risk. Further, in one agency, the audit committee structure supports the annual OMB A-123 assessment process by making recommendations to management with regard to the effectiveness of the system of internal control based on audit results and applying OMB A-123 definitions for significant deficiencies and material weaknesses. Drawing from private sector best practices, the composition of the audit committee includes senior management within the financial and IT functions as well as representatives from various mission-based programs to vet content prior to raising it for consideration by executive leaders. This integrated and multi-disciplinary approach has strengthened both the risk management and internal controls processes by ensuring a platform for detailed briefings on IT risk management, information security, and cybersecurity, using common enterprise risk criteria. Discussions include briefings on annual FISMA audit results, risk assessment reports, and cybersecurity enterprise risks. Meetings are held quarterly. The integration of an audit committee structure into the ERM governance structure has further correlated the outcomes and products of the required OMB A-130 and OMB A-123 processes.

### **Use Case (3)**

This federal agency's Office of Risk Management (ORM) serves as an independent office responsible for agency-wide risk functions, including ERM, agency-wide Information Security Risk Management (including Cybersecurity risk), and Continuity of Operations (COOP) programs. [The ORM supports the agency's senior level Risk Management Council](#). The agency's ERM program is relatively mature compared to its Information Security Risk Management (ISRM) program. Due to ORM's experience in implementing the agency's ERM program, it leads the effort, in coordination with the Office of the Chief Information Officer (OCIO) team (including the CISO who reports to the CIO), to develop and implement the agency's ISRM strategy program consistent with NIST guidelines, including NIST Special Publications 800-30, 800-37 and 800-39.<sup>76,77,78</sup> The first major outcome of this program was to create the agency's first comprehensive IT security risk register. With respect to ISRM risk, ORM facilitates the identification and assessment of agency's ISRM risks in coordination with the OCIO. The joint effort leverages the unique skill sets of ORM and OCIO for improved risk management processes.

Although the ORM and OCIO successfully work in coordination to address the agency's ISRM risks, it was

---

<sup>74</sup> [OMB A-123](#).

<sup>75</sup> [OMB M-19-03](#).

<sup>76</sup> NIST SP 800-30: Guide for Conducting Risk Assessments.

<sup>77</sup> [NIST SP 800-37r2: Risk Management Framework](#).

<sup>78</sup> [NIST SP 800-39: Managing Information Security Risk](#).

not without setbacks. The most difficult challenge to overcome was establishing boundaries between the roles of ORM and OCIO once the implementation phases began. For example, after the framework and strategy were complete, the ORM and OCIO held meetings for several months to distinguish the responsibilities each office would have in the establishment of its risk assessment method and creation of risk registers. Specifically, the OCIO pushed to ensure that, after jointly creating the agency's first ISRM registers with ORM, the offices each played a separate yet complementary role in managing the agency's ISRM risk functions in accordance with the tiered structure established in NIST: Organization level (Tier 1), Mission/Business Process (Tier 2) and System level (Tier 3).<sup>79,80</sup> In the end, it was determined that OCIO will address ISRM risks at Tiers 2 and 3, which includes creating a risk register, thereafter that risk register will feed into the ERM process and be integrated at the top tier (Tier 1) by the ORM.

Additionally, ORM is conducting the agency's business impact assessments (BIA) at the three Tiers in coordination with the OCIO. The BIAs will be used for contingency planning, which augments both the Business Continuity and Disaster Recovery (BC/DR) programs, and well as, the Continuity of Operations (COOP) function at the agency. The collaborative approach not only leverages the unique skill sets of both offices, but also avoids duplication of efforts for both the owners of the systems and OCIO and ORM personnel.

#### **Use Case (4)**

This agency has established an effective process for coordination between Cybersecurity and Enterprise Risk Management (ERM) through its ERM governance and operating structures. The agency's ERM program was established using the COSO ERM Integrated Framework as a guide. The agency created the Executive Risk Committee (ERC) and the Risk Working Group (RWG) as part of the ERM governance structure while integrating the ERM program into the agency's current operating structure. This integration helps ensure cyber risks are being considered by senior leadership in the context of other risks facing the agency.

The ERC is comprised of a small number of senior leadership members and oversees the identification, assessment, and management of enterprise risks, including cyber and security data risk. The agency's CIO is a permanent member of the ERC. Within the IT organization, the head of IT's Cybersecurity organization reports directly to the CIO.

The ERC assigns a Risk Owner to support the assessment of each enterprise risk. The Risk Owner is responsible for providing input for enterprise risk indicators and risk response strategies, and to also update the ERC on the current state of the risk, when requested. IT is the Risk Owner for various enterprise risks, including the cyber and data security risk. IT Cybersecurity provided an in-depth briefing to the ERC on cyber and data security risk during an ERC quarterly meeting and is expected to provide periodic briefings at future meetings.

The RWG supports the enterprise risk management process and the ERC. Members of the RWG include designated ERM Liaison representatives from all business units. The agency's IT's ERM liaison serves as a member of the RWG and interfaces between the Office of the Chief Risk Officer and IT, including Cybersecurity. ERM Liaisons work with their business unit leadership to evaluate business unit risks and

---

<sup>79</sup> NIST Special Publication 800-39, pg. 9.

<sup>80</sup> For this discussion, Tiers are synonymous with Levels illustrated in Figure 1.

submit business unit risk registers as part of the annual enterprise risk assessment. Data from the business unit level risk registers are aggregated, analyzed, and provided as input into the enterprise level risk report. IT's Risk Register, which includes input from Cybersecurity, serves as an input into the enterprise risk assessment. During the annual enterprise risk assessment, the RWG meets to review aggregated risk information and identify potential exposures and other information, such as risk response strategies, needed to enhance ERC understanding of the risk profile. IT Cybersecurity representatives participate in discussion of cyber-related risk information with the RWG.

### **Use Case (5)**

This government agency had an IT Material Weakness in its financial systems. The agency's independent auditor reported it over several decades ago and it persisted for many years. The problem was complex and pervasive across systems in a decentralized and federated environment. To solve the problem, the agency leadership initiated a comprehensive strategy in Fiscal Year (FY) 2015 that emphasized maturing the overall control environment, reducing security risks of financial systems, and resolving the IT Material Weakness.

Implementing this strategy required collaboration across functional areas from IT, information security, financial and programs areas within the agency. To set the "tone at the top" with cross-functional alignment, the agency and components' Chief Financial Officers (CFOs), Chief Information Officers (CIOs), and Chief Information Security Officers (CISOs) got together to establish this effort as a Departmental priority. They assigned dedicated resources to establish a cross-functional IT Material Weakness Working Group (IT MWWG), co-chaired by representatives from OCFO and the OCIO. Since its establishment, the group has been focusing on analyzing identified control deficiencies, tracking remediation efforts, and evaluating risks. The group has reported the remediation progress and risk results to CIO, CFO, and CISO communities, as well as governance boards. In FY2018, they were able to conclusively demonstrate the progress they have made; as a result, the auditor downgraded the long-standing IT Material Weakness to a Significant Deficiency.

This agency's focused efforts on resolving and downgrading their 23-year Financial IT Systems Material Weakness (cybersecurity risks in configurations management, access controls, separation of duties etc.) is a success story involving systematic thinking about risk reduction and collaboratively harnessing efforts to focus on targeted areas.

Key success factors include:

- Building management capabilities to identify, assess, and manage risks effectively.
  - Innovative "Management Assessment Framework" (MAF) tool: Building upon the best practices of the Government Accountability Office (GAO) high-risk program evaluation, "ERM risk de-elevation criteria," IT MWWG developed the MAF as a common set of criteria to evaluate risk systematically from governance, risk reduction, and demonstrate progress of security and controls maturity. It enables the agency's management assertion on its financial systems control environment to support management assurance process.
  - "Audit Readiness Playbook" to help communications with the auditor. The guide helps IT Systems' teams effectively communicate the systems controls to auditors and facilitate the risk discussion considering compensating controls. This is a good risk practice that helped everyone "reach a common view of risks" (another ERM principle) by bridging the communication gap between systems teams and auditors.

- Engaging stakeholders in a decentralized environment to increase risk awareness, understand the identified risks' potential impacts, and measure the progress of risk mitigation. The IT MWWG brought people together from across the Department to operating divisions among the CFO, CIO, and CIO communities to foster a risk-aware culture and led the transformation with common values shared through commitment, communication, connection, and collaboration.

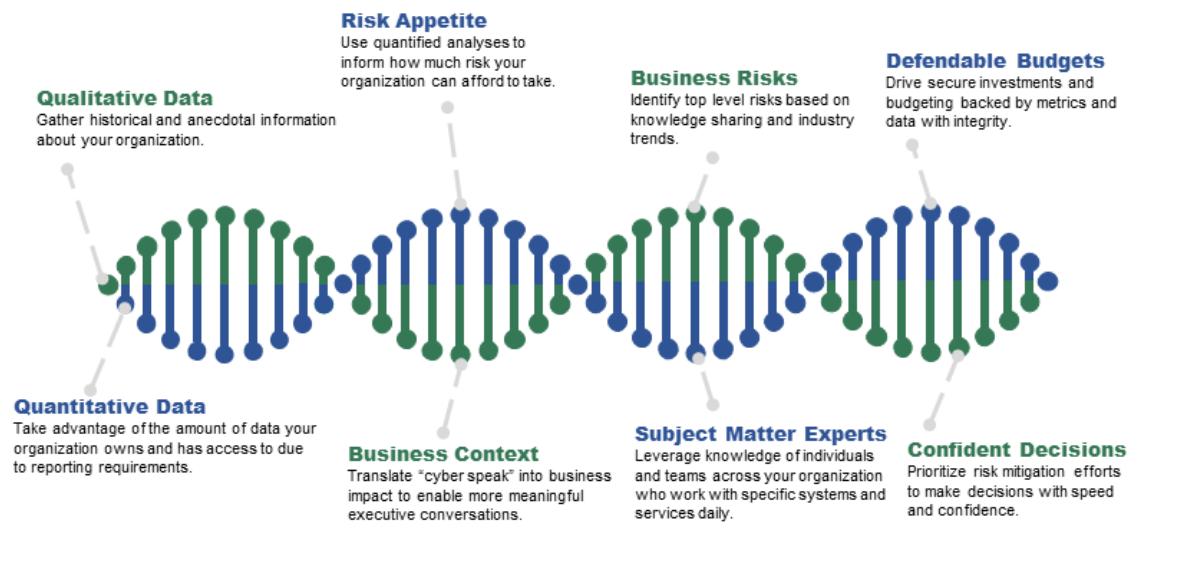
#### **Use Case (6)**

This agency's success story dates back to July 2018 for Cyber-ERM integration. One tip is to "just start talking with each other to find common ground." This federal agency helped sponsor, organize, and moderate a panel of experts across their agency and divisions for The Association for Federal Enterprise Risk Management (AFERM) at a lunch-and-learn event. This event had over 50 federal and contractor attendees and is believed to be one of the first times ERM professionals working in the Federal Government started talking about "getting started with integrating Cyber and ERM." Individuals who liked both Cyber and ERM were discovered and they collectively started talking about "communicating in plain language," "building relationships," "actively sharing information," "inviting each other to participate in the traditionally 'siloed' communities of practice," etc.

## L. Examples of Qualitative and Quantitative Risk Analysis Approaches

### Executing a Blended Approach

Using a blended quantitative and qualitative approach at each stage of risk management.



## CHALLENGES

### QUANTIFICATION OF MISSION OBJECTIVES

Quantifying loss magnitude or other components is difficult, particularly in cases of national security or protection of critical infrastructure. Traditional tactics of quantifying components such as loss of customers is not applicable.

**FOR EXAMPLE**, it is difficult to quantify the impact of the Office of Personnel Management (OPM) data breach in terms of loss to reputation. Instead, costs around additional personnel or credit monitoring services can be considered, but a change in perception of OPM and overall national privacy security is challenging to calculate.

### FLEXIBILITY & CUSTOMIZATION

Federal organizations are left to define their risk assessment approach on their own which can lead to inconsistent risk management methods across the enterprise.

### SUBJECTIVITY

Qualitative terms like "highly likely" or "high risk" are used inconsistently when not driven by quantitative measures.

### RANGE COMPRESSION & UNCERTAINTY

In a heat map, if three loss events have the same "Low" score but the expected loss ranges from \$50,000 to \$3M, it would be difficult to prioritize each risk appropriately if only the score is available. This limits the ability to make and defend recommendations or resource requests to address leadership business concerns.

### PRIORITIZATION WITH HEAT MAPS

#### SCENARIO Y

10% Likelihood x \$15M Impact  
= \$1.5M  
 $1 \times 3 = 3$

#### SCENARIO Z

75% Likelihood x \$2M Impact  
= \$1.5M  
 $3 \times 1 = 3$

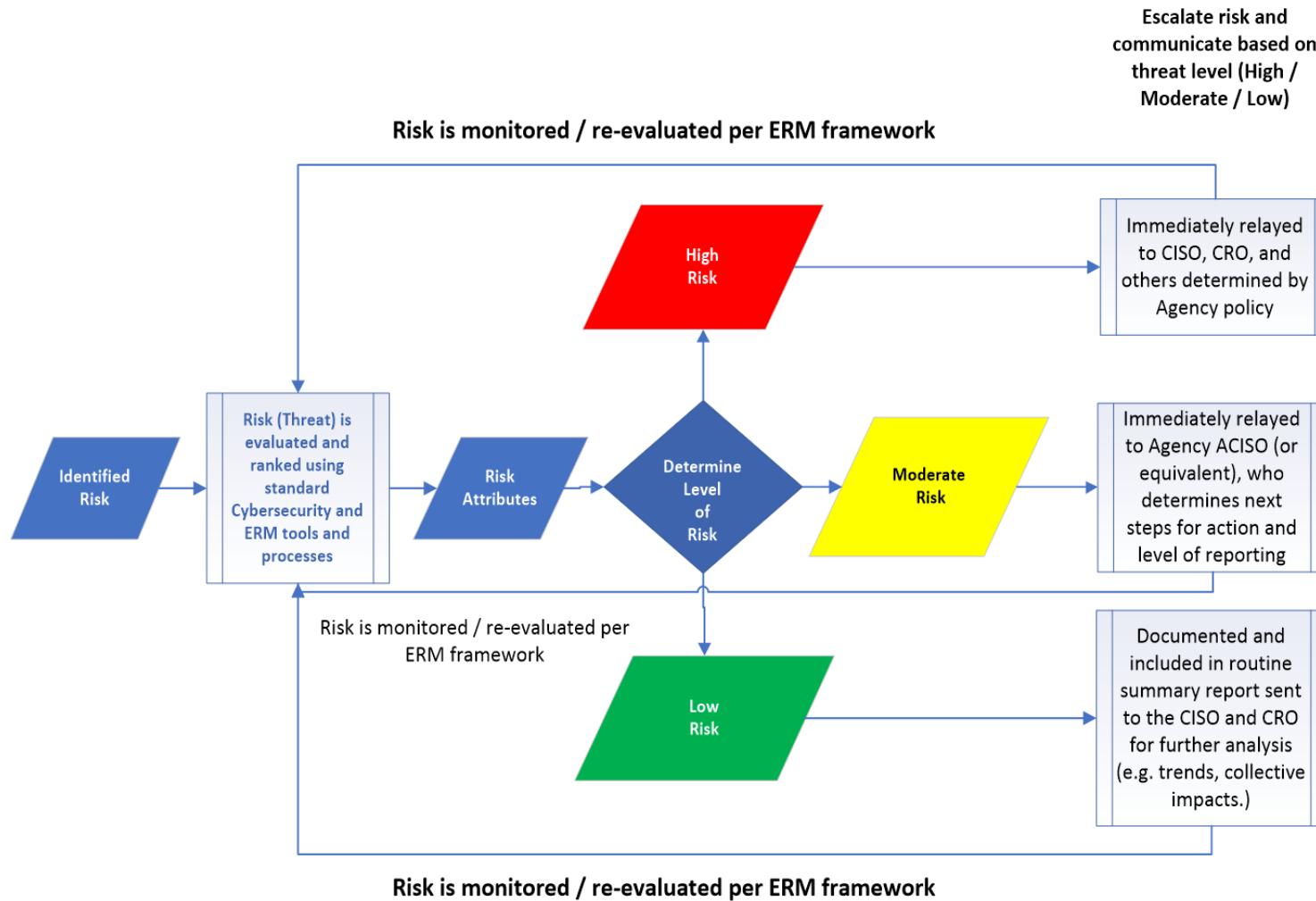
	4	4	8	12	16
Impact	3	(3)	6	9	12
	2	2	4	6	8
	1	1	2	(3)	4
		1	2	3	4
Likelihood					

**Challenge:** Although each scenario has the same estimated loss exposure, they fall on different priority levels (yellow vs. green) within the heat map.

## M. Examples of Roles and Responsibilities of Key Personnel for Effective Information Security and Cybersecurity Risk Management

Role/Title	Communication Responsibilities
Secretary / Deputy Secretary / Head of agency or designee	<ul style="list-style-type: none"> <li>• Communicates risk management messaging and policies across the organization regarding issues such as risks and information systems use policies.</li> <li>• Ensures Executive Branch visibility of high priority cyber risks affecting the federal landscape.</li> </ul>
Assistant Secretary with IT portfolio / Chief Operating Officer or equivalent	<ul style="list-style-type: none"> <li>• Provides and communicates strategic guidance on risk priorities affecting cybersecurity.</li> <li>• Determines Enterprise Risk Threshold (Tolerance), in consultation with the Chief Information Officer and Chief Information Security Officer, for high priority risk and ensures it is communicated and known by the appropriate staff.</li> <li>• Provides visibility of high priority risks to the Secretary and Deputy Secretary, or head of agency or designee.</li> </ul>
Chief Information Officer (CIO)	<ul style="list-style-type: none"> <li>• Communicates risk information, both situational and routine, to the Assistant Secretary for awareness.</li> <li>• Reports quarterly to the Secretary, Deputy Secretary, and Assistant Secretary / Chief Operating Officer, or equivalent, on the cyber risk posture.</li> <li>• Partner with Chief Risk Officer (peer-to-peer).</li> </ul>
Chief Information Security Officer (CISO)	<ul style="list-style-type: none"> <li>• Articulates and communicates the Risk Management Framework for the Department or agency to ensure the confidentiality, integrity, and availability of data, services, and information systems; serves as the driving force to make risk-based decisions to protect information systems.</li> <li>• Assesses submitted risk ratings to determine that risks are appropriately rated and communicates those risks to the CIO.</li> <li>• Partners with Chief Risk Officer or equivalent function using common enterprise risk criteria to translate the cybersecurity risk register to the enterprise level.</li> </ul>
Associate Chief Information Security Officer (ACISO) or equivalent	<ul style="list-style-type: none"> <li>• Ensures sub-organization staff are aware of policies and procedures to effectively manage Cybersecurity risks and balances risk with mission performance.</li> <li>• Coordinates with the CISO to document and track identified risks and provide additional information as needed.</li> <li>• Ensures risks are being monitored and periodically reports the status to the CISO.</li> <li>• Ensures risk responses are communicated back to the Risk Owner.</li> </ul>
Chief Risk Officer (CRO)	<ul style="list-style-type: none"> <li>• Captures key departmental strategic risks and provides information to leadership about those risks. overall agency impact in context to achieving of strategic goals.</li> <li>• Communicates on cybersecurity and information security risks in context of other enterprise risks to the established RMC and other stakeholders. Governing body for ERM. Supports translation to mission impacts.</li> </ul>

## N. Example of a Risk Communication Process Flow



## O. References and Resources

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

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

## P. Agency Acknowledgements

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

Name	Role	Agency
<b>Karen Weber</b>	Update Chair	Department of the Treasury (Treasury)
<b>William Bowman</b>	Editor/ Working Group	Veterans Health Administration
<b>Jill Lennox</b>	Editor/ Working Group	Federal Deposit Insurance Corporation (FDIC)
<b>Alex Wilson</b>	Editor	Treasury
<b>Piyavuth Bhutrakarn</b>	Working Group	Internal Revenue Service (IRS)
<b>Julie Chua</b>	Working Group	Department of Health and Human Services (HHS)
<b>Christopher Calfee</b>	Working Group	FDIC
<b>Maria Cruz</b>	Working Group	U.S. Agency for International Development (USAID)
<b>Karen Francis</b>	Working Group	Federal Retirement Thrift Investment Board
<b>Robin Funston</b>	Working Group	Department of Justice (Justice)
<b>Lori Giblin</b>	Working Group	Millennium Challenge Corporation
<b>Itzel Gonzalez</b>	Working Group	National Institutes of Health (NIH)
<b>Kim Isaac</b>	Working Group	Cybersecurity and Infrastructure Security Agency
<b>Nahla Ivy</b>	Working Group	National Institute of Standards and Technology (NIST)
<b>Eleni Jernell</b>	Working Group	Nuclear Regulatory Commission
<b>Jonathan Jones</b>	Working Group	HHS
<b>Daniel Kaneshiro</b>	Working Group	Office of Management and Budget (OMB)
<b>Daniel Lagriffe</b>	Working Group	Department of Energy
<b>Nancy Laurine</b>	Working Group	USAID
<b>Jacob Lee</b>	Working Group	Department of Interior
<b>Jason Leecost</b>	Working Group	Ginnie Mae
<b>Adam Lipton</b>	Working Group	OMB
<b>Lydia Lourbacos</b>	Working Group	Bureau of Safety and Environmental Enforcement
<b>Mary Marvin</b>	Working Group	Social Security Administration
<b>Curtis Masiello</b>	Working Group	Department of Defense (Defense)
<b>Curtis McNeil</b>	Working Group	Architect of the Capitol

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

<b>Alice Miller</b>	Working Group	U.S. International Development Finance Corporation
<b>Reginald Mitchell</b>	Working Group	USAID
<b>James Moore</b>	Working Group	Office of the Comptroller of the Currency (OCC)
<b>Thomas Moschetto</b>	Working Group	Treasury
<b>Nnake Nweke</b>	Working Group	U.S. Agency for Global Media (USAGM)
<b>Andrea Peoples</b>	Working Group	Small Business Administration
<b>Victoria Pillitteri</b>	Working Group	NIST
<b>Stephen Quinn</b>	Working Group	NIST
<b>Ahmad Rasuli</b>	Working Group	Treasury
<b>Melissa Reynard</b>	Working Group	IRS
<b>Nicole Rohloff</b>	Working Group	NIH
<b>Marianne Roth</b>	Working Group	Consumer Financial Protection Bureau
<b>Liz Ryan</b>	Working Group	Export Import Bank
<b>Christopher Smith</b>	Working Group	Defense
<b>Lenora Stiles</b>	Working Group	Treasury
<b>Kevin Stutts</b>	Working Group	FDIC
<b>Angelina Sulaka</b>	Working Group	USAGM
<b>Fahiem Usman</b>	Working Group	Treasury
<b>Joshua Vogel</b>	Working Group	General Services Administration
<b>Derrick Ward</b>	Working Group	Transportation Security Administration
<b>Debra Williams</b>	Working Group	Justice
<b>Jing Williams</b>	Working Group	HHS
<b>Montrice Yakimov</b>	Working Group	FDIC
<b>Jane Yang</b>	Working Group	Pension Benefit Guarantee Corporation
<b>William Rowe</b>	Contributor	OCC
<b>Neil Starzynski</b>	Contributor	Department of Labor

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