Association for Federal Enterprise Risk Management

Image by AzamKamolov from Pixabay

Federal ERM Areas of Practice Guidance – 2021

AFERM

Association for Federal
Enterprise Risk Management

Contents

Preamble

Association for Federal Enterprise Risk Management (AFERM) Federal ERM Areas of Practice Guidance 2021:

- Governance,
- ERM Maturity Model and Maturity Assessment,
- Risk Appetite Statement, and
- Establishing the Context.

This document is intended to provide guidance and is not meant to be an enforceable standard against which an agency ERM program is assessed. The key principles and subprinciples provided herein are intended to support and not conflict with requirements established by authoritative government entities such as the Office of Management and Budget, and guidance / recommendations provided through the Federal ERM Playbook. By design, these sources of government ERM program guidance provide agencies with significant flexibility and latitude to structure ERM programs to meet the unique mission, culture and needs of the organization. This document amplifies those government sources with key attributes associated with various Federal ERM areas of practice.

This guidance applies directly to ERM practitioners within U.S. Government Federal Agencies but may have broader application to agencies / organizations at other layers of government. The guidance is designed to provide practical information in the form of key attributes to assist ERM program leaders to develop or strengthen key aspects of their agency's ERM program. However, applying this guidance requires ERM program leaders to understand (1) key risk management principles, and (2) the distinction between risk management, ERM, and internal controls.

For the purposes of this document, risk management is defined as "a coordinated activity to direct and control challenges or threats to achieving an organization's goals and objectives."[1] This scope includes all objectives, whether they are strategically oriented and to be accomplished years in the future, executing a current business process daily, or ensuring accurate reporting or compliance with various organizational requirements. Historically, risks – even when managed well – have been managed within functional and program-specific areas of interest, and without regard to risks in other programs or functions. ERM is different.

AFERM defines ERM as "a discipline that addresses the full spectrum of an organization's risks, including challenges and opportunities, and integrates them into an enterprise-wide, strategically-aligned portfolio view." Of particular importance is the concept of a "portfolio" of risks, as ERM considers how to optimally balance various functional and programmatic risks across the enterprise for the benefit of the overall organization.

ERM also differs from and organization's internal controls program. Internal controls are an aspect of risk management focused on the control of risks in existing internal business processes and are thus a subset of traditional risk management. An internal control program becomes an element of ERM only to the degree that risk management within various functional and program "silos" is integrated into the organization's broader ERM program.

This document is focused on providing insight into the implementation of Federal ERM. However, such implementation builds upon the principles and practices of traditional risk management. The areas of Federal ERM practice thus include discussion of many traditional risk management approaches in addition to those that are exclusively associated with ERM, and are applicable to federal, state, and local governments.

[1] Definitions of Risk Management is found on page 107 of the *Playbook: Enterprise Risk Management for the U.S. Federal Government,* 2016 ed.

The value of this guidance will vary between Federal agencies and organizations based on several factors. These considerations include but are not limited to the type of organization (i.e., Department, major sub-component, independent agency, etc.); governance structure (e.g., single leader or a Board of Governors or Commissioners); organization size; level of ERM program maturity; placement of the ERM function within the organization; internal governance model; and the agency mission and strategy.

Background

The AFERM Vision is to *Be recognized as a credible authority and leader in promoting the effective application of enterprise risk management in the public sector*. Two of the Association's supporting Strategic Goals for 2020 – 2025 are to 1) Advance the Federal Government ERM Profession, and 2) Influence Federal Government ERM Practices. In support of these goals, the AFERM Board of Directors established a working group in October 2020 to evaluate and recommend whether the Association should develop an ERM Standard. Based on the working group recommendation, the Board approved moving forward on this initiative during the January 2021 monthly Board meeting.

To shape the development efforts of the working group, the Board approved 7 general design objectives. This document should:

1. Provide guidance on how to design and sustain an ERM program,
2. Be based on leading practices and publicly available documents,
3. Be applicable to a wide range of agencies varying in size, complexity, mission, and risk culture,
4. Define what is technically required and provide one or more methods where appropriate,
5. Be subject to Peer Review process,
6. Address the need to regularly update the portfolio of risks to respond to change in context, and
7. Be a living document updated as the state of ERM knowledge improves.

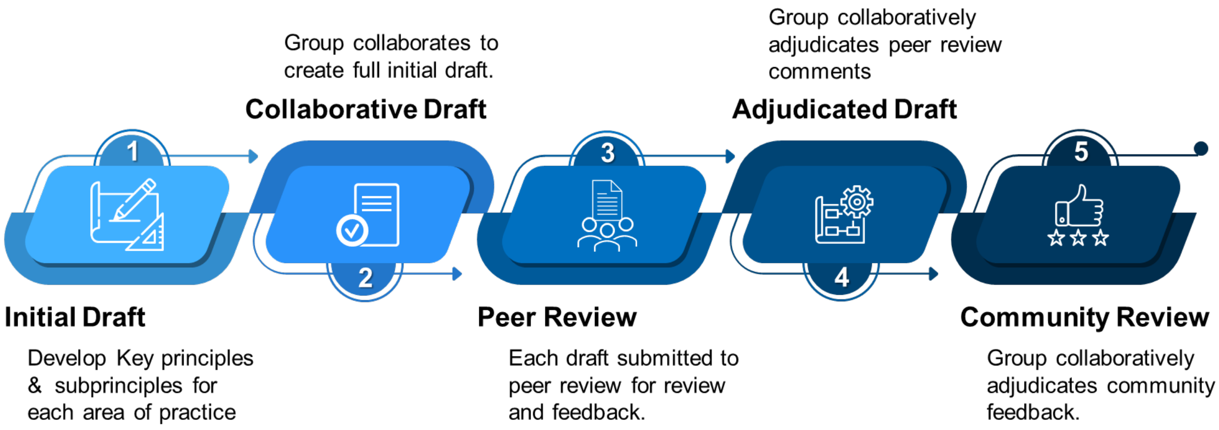
The underpinning for this effort is a common understanding that ERM programs are designed and operate according to the following principles:

- create and protect value,
- are based on the best information,
- are an integral part of organizational processes,
- are tailored,
- are part of decision-making,
- take human, cultural, and political factors into account,
- explicitly address uncertainty,
- are transparent and inclusive,
- are systematic, structured, and timely,
- are dynamic, iterative, and responsive to change, the velocity of change, and flow of information,
- facilitate continual improvement of the organization.

Development Approach

The Board recognized that developing guidance across all 20 Federal ERM areas of practice identified by the working group is a multi-year effort and set an initial goal to publish guidance on 4 areas of practice by the end of 2021. To achieve the 2021 goal, the working group selected areas of practice that are somewhat different between public sector and private sector organizations and for which there is limited publicly available information to guide ERM practitioners in the Federal sector. The areas of practice addressed in this 2021 release are: Governance, ERM Maturity Model and Maturity Assessment, Risk Appetite Statement, and Establishing the Context. The Board currently plans to develop guidance for additional areas of Federal ERM practice over the next several years.

For this initial 2021 release, each area of practice section went through 4 phases of development prior to publishing the draft document for general community review and comment, and a 5TH phase prior to approval by the AFERM Board.



1
Initial Draft
Develop Key principles & subprinciples for each area of practice
2
Collaborative Draft
Group collaborates to create full initial draft.
3
Peer Review
Each draft submitted to peer review for review and feedback.
4
Adjudicated Draft
Group collaboratively adjudicates peer review comments
5
Community Review
Group collaboratively adjudicates community feedback.

Federal ERM Areas of Practice Development Phases

Each area of practice section uses a common organizing structure beginning with a description of the area of practice and identifying the important attributes associated with the area of practice. For each identified attribute there is a brief description of what that attribute means; an explanation regarding why the attribute is important to an agency; examples of how an agency might achieve the attribute; example of different types of evidence for the attribute; and additional information relative to small agencies, where applicable.

The 5 members of the development working group included:

Daniella Datskovska
Doug Webster
Harold Barnshaw
Ken Fletcher
Paige Nicholson

Peer Review Process

The peer review process involved volunteers from across the Federal ERM community who are knowledgeable in the technical elements of a federal agency ERM program, are familiar with program design and operation, and are independent with no conflicts of interest that may influence the peer review process. The 12 peer reviewers were grouped into 3 teams comprising 2 federal employees and 2 non-federal individuals.

Peer review teams considered each section from the perspective on whether,

- the principles and subprinciples are relevant, sustainable, and scalable,
- the examples for how an agency might achieve the attribute and possible types of evidence are adequate to achieve the intent of the area of practice,
- the explanations and assumptions provided are reasonable, and
- the guidance is clearly stated to promote understanding.

Members of the Peer Review panel for 2021 included:

Marianne Roth
George Fallon
Stephanie Irby
Tom Brandt
Peggy Sherry
Tim Mobley
Bill Dykstra
Karen Weber
Chris Calfee
Rich Gallagher
Lewis Motion
Nicole Puri

Practice Area 1: Enterprise Risk Governance

1.1 Description All organizations seek to deliver value to their various stakeholders. Governance is "the act of governing or overseeing the control and direction of an organization"[2] in order to guide necessary decisions to deliver the desired stakeholder value. To achieve that objective, the governance structure aligns organizational efforts in setting direction, allocating limited resources, and managing risks. Enterprise risk governance provides the overall control and direction of risk management activities in a manner that maximizes organizational value. Specifically, the governing body ensures the organization identifies, assesses, treats, monitors, and communicates information about internal and external risks facing the organization that could enable or inhibit achieving key goals and objectives. While the management of risk within various functional and programmatic areas of the organization should respond to specific, localized needs to manage risk, the management of those functional and programmatic risks should inform an enterprise-wide risk governance process to ensure consistency with enterprise-level priorities.

The following principles and attributes contribute to design, implementation, and operating effectiveness of this area of practice:

- understanding what constitutes organizational value,
- transparency with internal stakeholders,
- accountability for risk-based decision-making,
- alignment of agency policy with statutory requirements and federal policy (OMB, OPM, GSA, etc.)
- strategic alignment,
- cross-organizational alignment,
- application of internal systems and controls, and
- risk information that informs agency decision-making.

1.2 Understanding what constitutes organizational value

1.2.1 Description: The agency determines and communicates what constitutes organizational value.

1.2.2 Explanation of Importance: All organizations exist to create value for their stakeholders and every management decision creates, protects, or erodes that value. Through enterprise risk management, agencies seek to implement a coherent approach to managing risks across the enterprise in a manner that contributes to protecting or creating stakeholder value. Without a clear understanding of what constitutes value, agency risk management efforts could be disjointed and misaligned resulting in the erosion of stakeholder value. The following considerations are helpful in developing the common understanding of what constitutes value for an individual agency:

- how legislation shapes the mission of the agency,
- how key stakeholders define value (relative to the mission of the agency), and
- how to balance opposing stakeholder interests to optimize the collective delivery of value to key stakeholders.

1.2.3 Examples of how agencies might achieve this attribute:

- establishing hierarchical decision-making processes that align risk decision-making vertically and horizontally across the organization,
- ensuring enterprise risk management decision-making processes benefit from transparent information flow through the organization relevant to risks faced and risk treatments considered and implemented,
- discussing with key external stakeholders their interests and needs, and
- promptly communicating changes in the direction of the agency to stakeholders.

1.2.4 Possible types of evidence and examples:

- meeting agendas/minutes,

[2] Merriam-Webster, https://www.merriam-webster.com/dictionary/governance

- agency budget,
- strategic plan, and
- committee charters.

1.3 Transparency with internal stakeholders

1.3.1 Description: The agency transparently communicates risk information to decision-makers impacted by those risks.

1.3.2 Explanation of Importance: Enterprise risk management seeks to manage risks consistent with a risk appetite that contributes to strategic direction and optimizing value. Transparent communication of risk information is an important element of the risk-informed decision-making process at all organizational levels and with individuals and components of the organization impacted by those decisions. Absent timely and relevant communication of risk information to inform decision-making, agencies may be ineffective in adequately managing risks and value becomes sub-optimal. Specifically, information on risks, to the extent known, should be conveyed to appropriate decision-makers regarding:

- risks identified to achievement of objectives relevant to the decision-makers,
- all relevant factors for analysis and evaluation of identified risks,
- considerations limiting choices on risk treatments to maximize portfolio value, and
- level of risk appetite appropriate for the objective and risk(s).

1.3.3 Examples of how agencies might achieve this attribute:

- adopt a process to convey appropriate information about risks to senior management and decision-makers across the organization, and
- provide specific written communication to impacted or concerned organizational stakeholders.

1.3.4 Possible types of evidence and examples:

- meeting agendas/minutes,
- risk profiles/registers, and
- risk heat map.

1.4 Accountability for risk-based decision-making

1.4.1 Description: The agency holds management accountable for appropriately managing risk to their operations.

1.4.2 Explanation of Importance: Risk is a part of all management decision-making, and it is important that decisions are aligned with and supportive of how the agency defines value and the amount of risk they are willing to accept. Without holding decision-makers accountable for ensuring an appropriate level of risk information informs decision-making, agency leaders cannot ensure appropriate alignment. Clearly communicated expectations from agency leaders regarding the accountability for risk-informed decision-making and incorporation of risk management into all day-to-day activities promotes effective risk governance.

1.4.3 Examples of how agencies might achieve this attribute:

- establishing and communicating clear roles and responsibilities for risk management within all parts of the organization,
- encouraging clear and open communication in discussing risks at all organizational levels,
- promoting communication across the organization to inform the decision-making process regarding risks present or resulting from potential decisions,
- establishing performance appraisal standards that require appropriate risk management practices, and
- documenting risks accepted as part of the formal documentation of goals and objectives.

1.4.4 Possible types of evidence and examples:

- performance standards that include accountability for risk management practices appropriate for each level of the organization (e.g., executive management; supervisors; front-line staff),
- inclusion of risk-management as part of agency management training, and
- individual and agency recognition for achievement in risk-based decision-making.

1.5 Alignment of agency policy with statutory requirements and federal policy

1.5.1 Description: Agency risk management policies align with statutory and administrative requirements.

1.5.2 Explanation of importance: A successful federal agency that meets mission and stakeholder needs requires alignment between internally generated organizational policy and externally imposed federal requirements. In addition to management failing in their compliance responsibilities, misalignment of organizational policy and regulatory requirements impedes identification and management of risks consistent with strategic direction and risk appetite.

1.5.3 Examples of how agencies might achieve this attribute:

- periodic review of organizational policies for consistency with regulatory requirements, and
- recurring review of risk appetite for consistency and alignment with organizational policies and regulatory requirements, and reconciling differences.

1.5.4 Possible types of evidence and examples:

- discussion of risk in agency planning initiatives (e.g., strategic plan), and influence of risk on resulting decisions and allocation of resources, and
- agency risk appetite statement with sufficient detail to guide decision-making.

1.6 Strategic alignment

1.6.1 Description: Agency leaders align risk management practices and reporting to manage risks to achieving agency strategic objectives and supporting line-of-business objectives.

1.6.2 Explanation of importance: Key enterprise risks to agency strategic objectives can originate in any line-of-business and at any level in the organization. A primary value to agencies from enterprise risk management is elevating those key risks from within organizational silos for visibility and management from an agency-wide perspective. Effective communication of enterprise-level risk information to senior managers and decision-makers facilitates decision-making that provides improved value to internal stakeholders. Without effective risk communication up through the organization, leadership is blind to agency risk exposure and cannot oversee and control the agency's response to ensure those risks are managed consistent with risk appetite. Strategic alignment also requires effective downward communication so that higher-level risk management decisions are effectively implemented and inform decision-making processes at lower levels of the organization. An effective risk governance structure promotes strategic alignment and consistent oversight of risk management activities across the organization.

1.6.3 Examples of how agencies might achieve this attribute:

- a structured governance process that communicates risks and actions taken to manage those risks vertically within lines-of-business to the extent needed to achieve risk-informed decisions and maximize overall organizational value.

1.6.4 Possible types of evidence and examples:

- establish/maintain a governance structure that ensures ongoing, reliable communication of risk management activities at all levels of the organization.

1.7 Cross-organizational alignment

1.7.1 Description: Agency leaders and managers actively communicate risk and risk treatment information across organizational boundaries and consider cross-organizational impacts in managing risks.

1.7.2 Explanation of importance: As with many types of decisions, the impact of risk management decisions can be felt at the programmatic, functional, and organizational levels. The agency risk governance process is most effective, and the benefits to the agency optimized, when cross-organizational impacts are considered and competing interests balanced to increase agency value. Doing so minimizes the potential for unintended or unanticipated consequences impacting other areas of the agency.

1.7.3 Examples of how agencies might achieve this attribute:

- a governance structure that includes inputs from all functions and programs of the organization,
- a risk management support structure that facilitates informal communication across the organization on risks and communicates findings to appropriate decision makers within the formal risk management governance process.

1.7.4 possible types of evidence and examples:

- an agency governance structure and process that receives inputs on cross-organizational risk considerations (threats and opportunities) and seeks to make decisions based on what most benefits the agency and its stakeholders, and
- documentation providing the rationale for any organizational element knowingly accepting greater or lesser risk within a functional or programmatic area to better optimize value at the agency level.

1.8 Application of internal systems and controls

1.8.1 Description: Agency leaders implement and oversee effective internal systems and controls to maintain reasonable assurance that the agency operates its internal business processes in a manner supporting delivery of desired outcomes.

1.8.2 Explanation of Importance: An agency's ability to optimize stakeholder value and achieve strategic objectives is underpinned by effective and efficient internal processes monitored through controls. One cause of enterprise-level risks is often weak or ineffective internal controls. By monitoring internal processes and the effectiveness of internal controls, the ability of the agency's risk governance structure to reduce the likelihood of a key risk occurring is enhanced.

1.8.3 Examples of how agencies might achieve this attribute:

- allow for the incorporation of significant internal control deficiencies into the organization's risk profile or register based on the level of control deficiency risk.

1.8.4 Possible types of evidence and examples:

- confirmation that all control weaknesses identified by internal or external auditors were considered by the governance process for incorporation into the agency risk profile.

1.9 Risk information informs agency decision-making

1.9.1 Description: Agency risk information is incorporated into all management decision-making processes in the organization.

1.9.2 Explanation of Importance: The integration of risk information into all decision-making processes supports the consistent delivery of risk-based decisions that appropriately balance considerations of results sought, resources allocated, and risks accepted. The incorporation and execution of risk management processes across the organization are essential elements supporting management decisions that optimize the delivery of stakeholder value.

1.9.3 Examples of how agencies might achieve this attribute:

- all components of the risk management process have been implemented consistent with documented agency policy,
- the necessary resources are allocated to managing risk, and
- authority, responsibility, and accountability for managing risk have been assigned.

1.9.4 Possible types of evidence and examples:

- review of programmatic, functional, and departmental policies as well as other documentation indicates management decision-making is informed by appropriate agency risk management practices.

Practice Area 2: ERM Maturity Model and Maturity Assessment

2.1 Description An ERM Maturity Model is a structured methodology that defines the key attributes, artifacts, and capabilities of an ERM program and describes those maturity elements along progressive levels of maturity (typically five (5) levels). Research shows a statistically significant positive relationship between ERM maturity and organizational value[3]. Considerably increasing ERM program maturity typically requires a multi-year effort. A well-designed ERM Maturity Model supports that effort and provides several broad benefits to an agency. The ERM Maturity Model:

- identifies multi-dimensional categories, processes, principles, attributes, and capabilities of importance to the agency's ERM program in a way that supports continuous improvement,
- provides a structure that allows the agency to pay attention to the desired future state of the program while focusing on specific aspects of maturity necessary to achieve that future state,
- provides a consistent and standardized gauge to periodically, thoughtfully, and objectively assess ERM program maturity, and
- supports multi-year program implementation and maturity planning.

An agency applies an ERM Maturity Assessment to a) **periodically evaluate the current state of ERM program maturity** against a maturity model and b) **identify the gap between the current and the desired state** of ERM program maturity to be achieved at a specified time in the future. The desired maturity state will differ for agencies depending on their size, mission and strategic objectives, culture, appetite for ERM, and other unique characteristics that influence the success and adoption of the ERM program. The path and the speed at which agencies achieve select levels of ERM program maturity will also depend on the amount of agency resources available to dedicate to the program. Agencies can use the results of an ERM program Maturity Assessment to:

- create a pragmatic roadmap to reach desired maturity levels by identifying areas for improvement and gaps to address,
- objectively measure success in achieving desired levels of maturity at each of the selected categories, and
- engage key stakeholders and further acceptance of the ERM program through a common "ERM language."

The following principles and attributes contribute to design, implementation, and operating effectiveness of this area of practice:

- incorporate key elements and attributes of an effective ERM program,
- plan and prepare for an ERM maturity assessment,
- execute the ERM maturity assessment, and
- define expected results and next steps.

2.2 Incorporate key elements and attributes of an effective agency ERM program

2.2.1 Description: The agency identifies, socializes, and approves ERM Maturity Model multi-dimensional categories and attributes. Some of the suggested categories for a multi-dimensional ERM Maturity Model are Risk Governance, Integrating Risk with Strategy and Performance, ERM Operating Model, Risk Management Process (Risk Identification and Assessment, Risk Response, Risk Monitoring and Reporting), Risk Culture, Risk Appetite, Risk Tools and Technology.

2.2.2 Explanation of Importance: An ERM Maturity Model is an important component of an agency's ERM framework and serves several key objectives. Most directly, the maturity model assesses the processes, the principles, categories, attributes, and capabilities of importance to the agency's ERM program and provides a measurement tool to objectively assess these ERM program elements. The

[3] Ertan, Y., (2017), *The Effect of Enterprise Risk Management Maturity Level on Financial Performance: The Turkish Case*; Proceedings of 66th IASTEM International Conference, Munich, Germany, 2nd -3rd August 2017: https://www.worldresearchlibrary.org/up_proc/pdf/998-15048619038-9.pdf

successive levels of maturity for these important program elements also provide a roadmap for increasing ERM program maturity to realize the desired future state and to communicate the value of the program to agency leaders.

Another key purpose of the maturity model is to keep in focus the foundational attributes and capabilities associated with an effective ERM program (e.g., Risk Governance, Integrating Risk with Strategy and Performance, ERM Operating Model, Risk Management Process, Risk Culture, Risk Appetite, Risk Tools and Technology). These attributes should be established at the lowest maturity level and each subsequent level should build upon them. This is important to maintain consistency and focus on the essential, foundational elements of the program and to avoid erosion of the value of ERM.

2.2.3 Examples of how agencies might achieve this attribute:

- include common multi-dimensional ERM maturity categories / attributes / processes / success factors suggested above or from an existing model from a credible source (e.g., ERM Playbook, OECD, RIMS, COSO etc.),
- adopt and customize the application of the model and path to achieving certain capabilities in the ERM Maturity Model, and
- confirmation of an ERM Maturity Model with agency leaders and key stakeholders.

2.2.4 Possible types of evidence and examples:

- agency's ERM Maturity Model.

2.3 Plan and prepare for an ERM Maturity Assessment

2.3.1 Description: The agency defines a plan for ERM Maturity Assessment execution, key process participants and inputs.

2.3.2 Explanation of Importance: Preparing for an ERM Maturity Assessment is a significant contributing factor to the success and the effectiveness of the assessment itself. A well planned ERM Maturity Assessment delivers value by providing insights into maturity gaps. It also increases awareness and acceptance of the agency's ERM efforts by strengthening program support from existing ERM program champions and by gaining new ERM champions. The ERM Maturity Assessment planning phase helps define key project roles and responsibilities, project milestones and deliverables. It also facilitates the examination and evaluation of current agency practices, policies, procedures, and communications that relate to ERM.

2.3.3 Examples of how agencies might achieve this attribute:

- development of project management and communication plans,
- kick-off project,
- examine and evaluate existing agency documents on risk management and ERM, governance structure, technology and budget and performance goals,
- gain an understanding of the agency's ERM Maturity Model,
- validation of assessment questionnaire,
- definition of assessment distribution mechanism, i.e., interviews/workshops/survey,
- identification and selection of assessment stakeholders,
- identify appropriate leading practices,
- discussion with agency leaders, and
- communication announcement of an assessment from agency leadership.

2.3.4 Possible types of evidence and examples:

- document request form,
- communication plan,
- project plan,
- assessment questionnaire, and
- list of select key stakeholders.

2.4 Execute ERM Maturity Assessment

2.4.1 Description: The method by which an ERM Maturity Assessment is carried out depends on several factors, including but not limited to the size of an agency, participants' familiarity with the subject matter, organizational culture around assessments and the frequency and timing of other assessments.

2.4.2 Explanation of Importance: Executing an evidence based ERM Maturity Assessment will provide the information necessary to evaluate strengths, weaknesses, and opportunities for the ERM Program. The results of a maturity assessment help agencies identify potential gaps between their current and desired states of maturity and help to thoughtfully plan for achieving ERM maturity at a desired pace and level.

2.4.3 Examples of how agencies might achieve this attribute:

- analyze collected information,
- administer the assessment considering the following:
    - if conducting interviews, analyze information gathered during the planning phase to develop context for stakeholder discussions,
    - surveys can be a useful tool for large audiences or when anonymity is important, and
    - assessments by individual stakeholders allow for the gathering of individual viewpoints; whereas group assessments allow for open discussion and reaching immediate consensus on ratings."
- document current state, including a mapping of how risks are monitored and managed today,
- compare as-is risk capabilities to leading practices,
- assess the effectiveness of current ERM practices against benchmark data and criteria,
- discuss initial results with agency sponsor to receive feedback and fine-tune conclusions, and
- complete the ERM Maturity Assessment with notes/inputs captured from interviews or group sessions.

2.4.4 Possible types of evidence and examples:

- assessment matrix with current state description and ranking against the maturity scale.

2.5 Define expected results and next steps

2.5.1 Description: The agency determines the gaps between current and desired state and defines its ERM roadmap to ERM program maturity.

2.5.2 Explanation of Importance: The results of an ERM Maturity Assessment will help establish the current state of ERM program maturity, identify the target state ERM capabilities and the gaps between the current and the desired state. At the end of the maturity assessment, the agency defines improvement opportunities that are aligned with leading practices and leverages current ERM processes. The results of the assessment also help identify potential integration points between ERM opportunities and existing business processes (e.g., strategic planning and reviews, internal control, budgeting, and performance management).

2.5.3 Examples of how agencies might achieve this attribute:

- identify and prioritize risk management objectives, key integration points and improvement opportunities,
- confirm findings and ensure inclusion of all relevant data and materials,
- produce an objective evaluation of current ERM/risk management practices, and
- conduct briefing with stakeholders.

2.5.4 Possible types of evidence and examples:

- high-level ERM maturity road map and the summary report.

Practice Area 3: Risk Appetite Statement

3.1 Description Risk appetite is 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.[4] A clearly defined, written and well-communicated risk appetite statement (RAS) provides alignment vertically and horizontally across an agency regarding the type and amount of risk that agency leadership has determined to be acceptable. The RAS helps employees make informed decisions regarding how to respond when addressing questions of policy, allocation of resources, the design and execution of internal controls, and in establishing performance targets and boundaries of acceptable performance variation. The statement can also help external stakeholders better understand agency actions in the context of the risks facing the organization. A well-defined process to develop a risk appetite statement helps agency leaders and managers:[5]

- better manage and understand their risk exposure,
- make informed risk-based decisions,
- understand risk/cost/benefit trade-offs, and
- identify opportunities to pursue to increase value.

The following principles and attributes contribute to design, implementation, and operating effectiveness of this area of practice:

- considers the agency context,
- considers the agency strategic goals,
- involves key internal stakeholders,
- written document approved by the agency leader,
- reviewed regularly and updated, when necessary, and
- provides guidance / expectations for use.

3.2 Considers Agency Context

3.2.1 Description: Agency leadership considers the agency context when establishing risk appetite.

3.2.2 Explanation of Importance: How an agency manages its key internal and external enterprise risks is influenced by the risk context in which the agency operates. To make the RAS meaningful and useful to decision makers it must take into consideration the unique mission and operating environment of the agency which are critical elements of context. An RAS that does not take into consideration the appropriate context can impede or diminish the effectiveness of agency programs and processes. A single risk appetite level may provide insufficient guidance and different risk appetite levels may be appropriate for different areas of risk exposure. This multi-dimensional approach can occur at different layers with the agency's risk taxonomy with different appetite for different risk categories (Layer 1), for subcategories (layer 2), or within sub-subcategories (layer3) – or for different aspects of agency operations.

3.2.3 Examples of how it might be achieved:

- discussions with agency leaders,
- discussions with key external stakeholders (e.g., other federal agency partners, FACA[6] committees, industry trade groups, mission implementing partners),
- review of administration policy documents (e.g., Executive Orders, OMB memorandum),
- review of congressional authorizing legislation and appropriations language,

[4] Playbook: Enterprise Risk Management (ERM) for the Federal Government (2016) pp 107

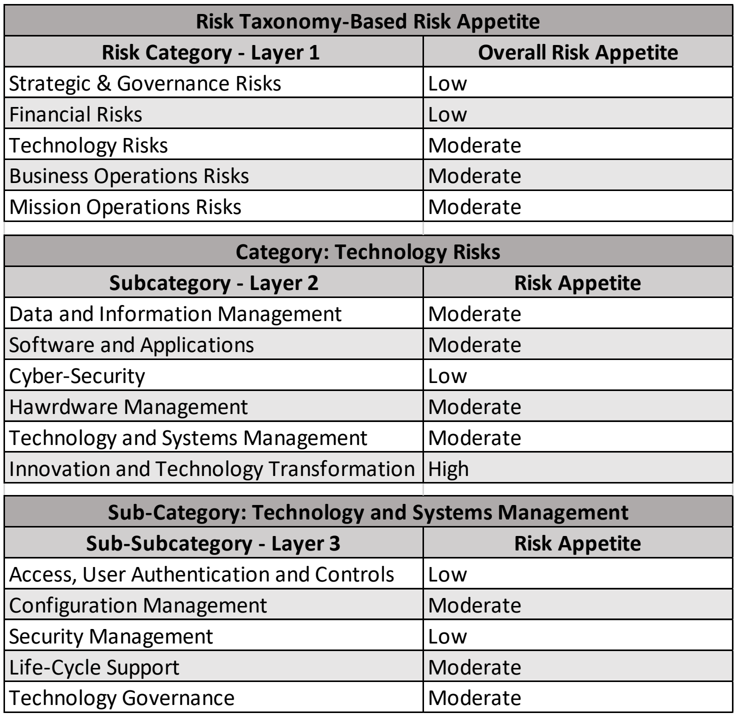
[5] North Carolina State University - https://erm.ncsu.edu/library/article/understanding-risk-appetite

[6] Federal Advisory Committee Act

- review of relevant Federal and industry guidance on RAS,[7] and
- review of GAO and other reports (such as the High-Risk List) and any audit findings relevant to the agency's risk landscape.

3.2.4 Possible types of evidence and examples:

- meeting / discussion minutes,
- meeting agendas,
- agency specific executive orders,
- briefings for authorizing and appropriation committee members and staff,
- agency priority goals and cross cutting performance goals, and
- multi-dimensional Risk Appetite Statement (see Example 3-1).



Risk Taxonomy-Based Risk Appetite	
Risk Category - Layer 1	**Overall Risk Appetite**
Strategic & Governance Risks	Low
Financial Risks	Low
Technology Risks	Moderate
Business Operations Risks	Moderate
Mission Operations Risks	Moderate

Category: Technology Risks	
Subcategory - Layer 2	**Risk Appetite**
Data and Information Management	Moderate
Software and Applications	Moderate
Cyber-Security	Low
Hawrdware Management	Moderate
Technology and Systems Management	Moderate
Innovation and Technology Transformation	High

Sub-Category: Technology and Systems Management	
Sub-Subcategory - Layer 3	**Risk Appetite**
Access, User Authentication and Controls	Low
Configuration Management	Moderate
Security Management	Low
Life-Cycle Support	Moderate
Technology Governance	Moderate

Example 3-1

3.3 Considers Agency Strategic Goals

3.3.1 Description: Agency leadership considers strategic goals when developing the RAS.

3.3.2 Explanation of Importance: Through the RAS, agency leadership broadly defines the amounts and types of risk exposure agency leaders are willing to accept in pursuit of its mission and strategic goals and objectives. Considering strategic goals and objectives when developing the agency's RAS helps integrate and align risk appetite with the organization's direction. Establishing this alignment helps

[7] Relevant guidance could include:
International: COSO ERM Integrated Framework; ISO 31000; UK Orange Book
Federal: OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control; GAO-17-63 Enterprise Risk Management; GAO-14-704g Standards for Internal Controls in the Federal Government ("GAO Green Book"); Chief Financial Officers Council Playbook: Enterprise Risk Management for the U.S. Federal Government ("ERM Playbook"); Office of Inspector General (OIG), Council of the Inspectors General on Integrity and Efficiency (CIGIE) – Inspectors General Guide to Assessing Enterprise Risk Management
Industry: NC State Poole College of Management – Enterprise Risk Management Initiative

guard against the potential that the agency's actual risk exposure undermines achieving those goals and objectives. Similarly, considering risk appetite when developing agency strategic goals and objectives helps ensure strategic initiatives fall within the boundaries of acceptable risk. Risk and strategy are complementary, and each should be considered when developing the other.

3.3.3 Examples of how it might be achieved:

- explicitly addressing strategic goals and objectives in the RAS,
- organizing the RAS around the agency's strategic goals and objectives,
- describing how the RAS works to support the agency's strategic goals and objectives,
- aligning strategic decisions with the RAS, and
- integrating RAS with performance measures / metrics.

3.3.4 Possible types of evidence and examples:

- Risk Appetite Statement.

3.4 Involves Key Internal Stakeholders

3.4.1 Description: Agency leadership involves key internal stakeholders when establishing risk appetite.

3.4.2 Explanation of Importance: The RAS is intended to enhance agency performance and control risk exposure in a way that supports agency goals and objectives and the priorities of agency leaders. The robust discussions and consensus achieved through engaging key internal stakeholders during RAS development produces a final product that benefits from diverse perspectives and insights. As a result, the final RAS is more meaningful to agency employees as it represents the insights, knowledge, buy in, and experience of a broad spectrum of agency leaders and is more likely to be adhered to because of their involvement.

3.4.3 Examples of how it might be achieved:

- governance meetings, and
- interviews and discussions.

3.4.4 Possible types of evidence and examples:

- minutes of governance meetings,
- notes or minutes from leadership interviews, and
- notes or minutes from leadership discussions.

3.5 Written Document Approved by Agency Leadership

3.5.1 Description: Agency head approves the risk appetite statement.

3.5.2 Explanation of Importance: The RAS provides guidance and direction from the agency leader on how employees should think about and manage risks within their respective jobs. Without the approval of the agency's leader a disconnect could exist between the direction the leader wants to take the organization and how risks are managed across agency operations and programs. Such a disconnect could lead to missed strategic opportunities, and risks managed in ways that undercut the policy, strategic and operational priorities of the leader of the agency.

3.5.3 Examples of how it might be achieved:

- approval record is documented in the agency policy approval process,
- the RAS is physically signed by the agency head,
- agency leadership issuing a directive promulgating the RAS, and
- RAS included in the strategic plan.

3.5.4 Possible types of evidence and examples:

- signed RAS document,
- policy approval document, and
- promulgation directive,

3.5.5 Small Agency Consideration: For small agencies and agencies with a board of Governors, Commissioners or Directors, the RAS can be approved by the Chief Operating Officer (COO), Chief Financial Officer (CFO) or another designated agency executive. It is a good practice to discuss the RAS with the Board for concurrence and to modify as necessary to incorporate board input.

3.6 Reviewed and Updated Regularly

3.6.1Description: Agency leadership regularly reviews and updates the Risk Appetite Statement.

3.6.2 Explanation of Importance: The RAS should be reviewed at regular intervals and after triggering events to ensure it remains appropriate to the current environment (see Example 3-2). As risk context changes the amount and type of risk agency leaders are willing to accept may also change. If the RAS is not reviewed and updated following a significant change in context, it may begin to work against the needs of the agency and become a less meaningful tool in facilitating achievement of mission objectives.

3.6.3 Examples of how it might be achieved:

- establish policy requirement for periodic review of the RAS,
- incorporate RAS review as a standing Risk Management Council (RMC) agenda topic (or equivalent governance entity), and
- determine the events that would trigger RAS review.

3.6.4 Possible types of evidence and examples:

- revision memorandum,
- table of review and changes,
- reissued RAS,
- agency-wide communications of changes to the RAS,
- Risk Management Council (or equivalent governance entity) minutes, and
- policy for periodic review following triggering events (see text box example). [8]

> **Example**: Certain key events have the potential to fundamentally alter the Agency's risk context and should prompt a review and update (as necessary) of the Risk Appetite Statement (RAS). The impact of these triggering events on the agency's RAS may not become apparent until sometime after the fact. These triggers may include:
>
> - Change in Presidential Administration
> - Change in key agency leadership (e.g., Secretary, Deputy Secretary, Director, Deputy Director etc. …)
> - External mandate from Congress or the Administration affecting the Agency's risk management processes, or which increase or decrease risk exposure for major programs.
> - Following a significant risk event which had a major or extreme impact on the Agency.

Example 3-2

[8] Example adapted from the Defense Logistics Agency

3.7 Provides Guidance / Expectations for Use

3.7.1 Description: Agency leadership includes clear guidance and/or expectations on how employees should use the RAS.

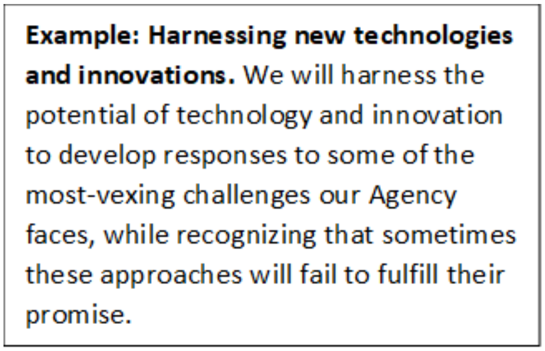
3.7.2 Explanation of Importance: The RAS creates a foundation for effective communication and understanding of risk and risk response posture among agency employees. The RAS provides a clear articulation of the agency's risk-response philosophy regarding specific types or categories of risk.

3.7.3 Examples of how it might be achieved:

- RAS contains section on how to use the document,
- descriptions of risk management strategies for different types of risks, and
- RAS aids in determining the type of response (e.g., avoid, pursue, mitigate, transfer etc..) for different types of risks.

3.7.4 Possible types of evidence and examples:

- Risk Appetite Statement (see Example 3-3).[9]



Example: Harnessing new technologies and innovations. We will harness the potential of technology and innovation to develop responses to some of the most-vexing challenges our Agency faces, while recognizing that sometimes these approaches will fail to fulfill their promise.

Example 3-3

[9] Example adapted from USAID Risk Appetite Statement

Practice Area 4: Establishing the Context

4.1 Description Understanding the risk management context is foundational to the effectiveness of any ERM program. The importance of establishing the context is indicated by its placement as Step 1 in the risk management process described in the ERM Playbook and the precursor of the risk assessment process in ISO 31000. Broadly, context is "the interrelated conditions in which something exists or occurs." External to the organization, these interrelated factors are legal and regulatory requirements; domestic and international economic and market conditions; stakeholder expectations; Administration policies and priorities; geo-political considerations; implementing partners; third-party service providers; and other government agencies. Combined, the external context enables or constrains an agency's ability to accomplish its purpose and achieve its strategic goals and objectives. Contextual factors internal to the organization include organizational culture; governance structure; policy and rulemaking processes; leadership appetite for risk; and the agency's execution strategy and supporting processes, strategic goals and objectives. These internal factors inform what risks the agency is willing to take and how an agency responds to the risk events it encounters.

Through establishing the context, the organization works to understand its operating environment and is better prepared to avoid unforeseen events and pursue opportunities that preserve or create value to the American people. The organization determines objectives and identifies the internal and external factors influencing the risk management process. This is an iterative process as the objectives and factors that can influence the way in which an organization will manage risk will change over time. By establishing the context, an organization aligns the goals and scope of the risk management process with the internal and external environment within which it operates.

There is no one truth in establishing the context. The value is in the process and the understanding that everything in the world is changing. It's a kaleidoscope. An agency should adjust decisions about risk as new information becomes available. Establishing the context should inform an agency's internal management discussions and prioritization of goals and objectives.

Establishing the context is a similar process in public and private institutions. The difference lies in what the entities can do in response to what they learn. Appropriated federal agencies have missions shaped by legislation and operate under long budget cycles. Agency leadership cannot go to a bank to borrow money or access financial markets to raise funds to pursue opportunities. Agencies have little flexibility to support major new activities and related risks beyond what is legislatively required. In contrast, private sector firms are driven by the desire for financial gain. In managing risk, a firm balances risk and return so that a firm enhances value to itself and its owners. A firm can raise additional capital through debt and equity financing to make considerable changes in its business over time in order to take advantage of constantly changing market conditions.

The following principles and attributes contribute to design, implementation, and operating effectiveness of this Federal ERM practice area:

- objectives of the organization and the constraints within which it operates,
- internal and external environment of the organization, and
- risk criteria set by agency leadership.

4.2 Considers Objectives and Constraints

4.2.1 Description: Agency leadership considers the objectives of the organization and the constraints within which the entity operates when establishing the context.

4.2.2 Explanation of Importance: Every agency has organizational objectives and constraints specific to their mission and strategy. Organizational objectives, established through a thoughtfully considered and strategically aligned planning process, serve as the basis for identifying risks and constraints to achieving those objectives. It is essential to understand the governing legal and regulatory compliance requirements as they form the foundation of the agency's objectives and are a key source of constraints. Ultimately, agency leaders should modify the risk management process to support the achievement of these objectives given the constraints, wherever they may originate.

While the measures of success for a commercial sector entity are economic viability and shareholder value, evaluating the success of federal agencies is significantly more complex. The standards on which federal agencies are judged are based on legal and political priorities, and public acceptance and support for the way in which the agency executes its mission. Economic viability and shareholder value do not determine the fate of most agencies and the decisions made by agency leadership in executing their responsibilities might make little sense to those motivated primarily by profit.

4.2.3 Examples of how it might be achieved:

- clearly articulated agency mission and objectives,
- review of legislative requirements applicable to the agency, and
- alignment of resources and priorities consistent with legislative requirements.

4.2.4 Possible types of evidence and examples:

- mission statement,
- vision statement,
- list of core values,
- inventory of applicable legislative requirements,
- budget, and
- strategic plan.

4.2.5 Small Agency Consideration: Revenue sources and cost of programs will likely have an outsized influence on the environment in which the agency operates and the constraints it faces.

4.3 Considers the Internal and External Environment

4.3.1 Description: Agency leadership considers the internal and external environment of the organization when establishing the context.

4.3.2 Explanation of Importance: The internal and external environment forms the context in which the agency operates to achieve its mission and objectives and shapes the way risks are managed. An agency that lacks an understanding of both the internal and external context is less likely to have an effective risk management process. Understanding the internal and external context is a dynamic endeavor because neither environment is static. When changes occur in the internal or external environment, agencies should reassess strategic planning assumptions which may be no longer valid and adjust operations appropriately. The complexity and nature of the agency's mission will often determine the number of internal and external factors that leadership needs consider when establishing the context.

Developing an accurate understanding of the internal and external environment and avoiding the compartmentalization of risks requires agency leaders to have an end-to-end understanding of transactions and supporting processes and the willingness to share information. Otherwise, an agency will be unable to determine if its internal controls infrastructure aligns with its risk appetite and supports agency objectives. This end-to-end business process understanding also helps leadership identify agency dependencies, along with the roles and importance of implementing partners and third-party service providers to overall agency success.

4.3.3 Examples of how it might be achieved:

- assess the legal and regulatory environment,
- consider political priorities of the administration and congressional oversight bodies,
- establish a risk-informed culture and collaborative management team to monitor risk across the enterprise, including third-party service providers,
- assess the agency's extended enterprise (e.g., reliance on partner organizations, influence of employee bargaining groups),
- consider stakeholder needs and expectations and identify any misalignment with agency mission and objectives,

- recognize capabilities, limitations, and risk exposure of implementing partners,
- assess the stability of administrative policy, the availability of resources, and public acceptance of agency actions,
- understand the impact of “tone at the top” on the agency’s culture and risk appetite, and
- assess the understanding and application of the agency’s risk appetite in formulating management decisions.

4.3.4 Possible type of evidence and examples:

- sources of risk to the agency,
- organizational structure and processes to achieve objectives and manage risk, and
- stakeholder analysis.

4.3.5 Small Agency Considerations: Small agencies may find it difficult to staff appropriately to manage risk. These agencies are often heavily reliant on third party service providers for operational support, which may limit flexibility when managing risk.

4.4 Set Risk Criteria

4.4.1 Description: Agency leadership sets risk criteria when establishing the context.

4.4.2 Explanation of Importance: Setting risk criteria provides clear guidance and a repeatable process for evaluating the significance of identified risks to the organization from a wide variety of sources. The criteria should support a consistent approach to identification, assessment, and prioritization of risks, including current and emerging risks, to the agency. Assessing risks without providing the necessary criteria and guidance will likely lead to problems prioritizing risks and allocating agency resources to manage them and inhibit agency leadership in taking appropriate action to safeguard or adjust goals, objectives, and strategies.

Because the context is constantly changing, agency leadership should have a process in place to adjust risk criteria when warranted. The particulars of certain criteria and the relative priority of different criteria might change when, for example, there is a change in Presidential Administration.

4.4.3 Examples of how it might be achieved:

- determine how the agency will measure negative events and assess uncertainty in objectives, the internal and external environment, and capabilities,
- define likelihood,
- determine levels of inherent and residual risk,
- determine risk appetite,
- develop a process to aggregate risks,
- hold managers accountable for making prompt decisions about risk and uncertainty (i.e., accept risk, share risk, reduce risk, avoid risk), and
- regularly review risk decisions and their relationship with risk criteria and risk appetite to support alignment.

4.4.4 Possible types of evidence and examples:

- risk evaluation criteria,
- risk impact criteria, and
- risk acceptance criteria.

4.4.5 Small Agency Considerations: Fee-funded agencies dependent on one or two programs for most of its revenue may be limited in their ability to take risk.