Enterprise Risk Management Assessment for the Project Management Agency

Your Task

The Project Management Agency (PMA) has been building an enterprise-level risk capability for the past two years and is now looking for an independent assessment of its progress. PMA is a federal agency responsible for research and development in various sectors: national defense, energy, and space exploration being the biggest. PMA currently consists of a headquarters office, five program offices, and three research centers. The leadership at PMA is planning a reorganization that will take effect on January 1, 2020, and wants to make sure that risk management is considered.

At the start of fiscal year 2018, PMA developed its initial Enterprise Risk Management (ERM) program. A Risk Management Working Group was chartered and began drafting the PMA Risk Management Plan. That plan includes the requirement that risk be included in all program and project reviews. As of October 2019, the Risk Management Plan has not yet been approved. The Risk Management Working Group assigned a Risk Manager, working at the headquarters level, to be responsible for the evolving ERM capability. Senior leadership created a Risk Management Board to ensure risk is addressed in the PMA Strategic Plan and to approve changes suggested by the Risk Management Working Group.

The Risk Manager has asked your team to assess the current state of PMA's ERM program. Your analysis should include a determination of compliance against relevant regulations and an evaluation of ERM maturity across competency areas, identifying strengths, weaknesses, and gaps. Your deliverable for this project is a briefing that your team will present to a group of senior leaders at PMA. The briefing must include, at a minimum, the following:

- assessment of the current ERM program,
- actionable steps to address non-compliance,
- recommendations for advancing ERM maturity, and
- prioritized risk management areas for improvement.

Background

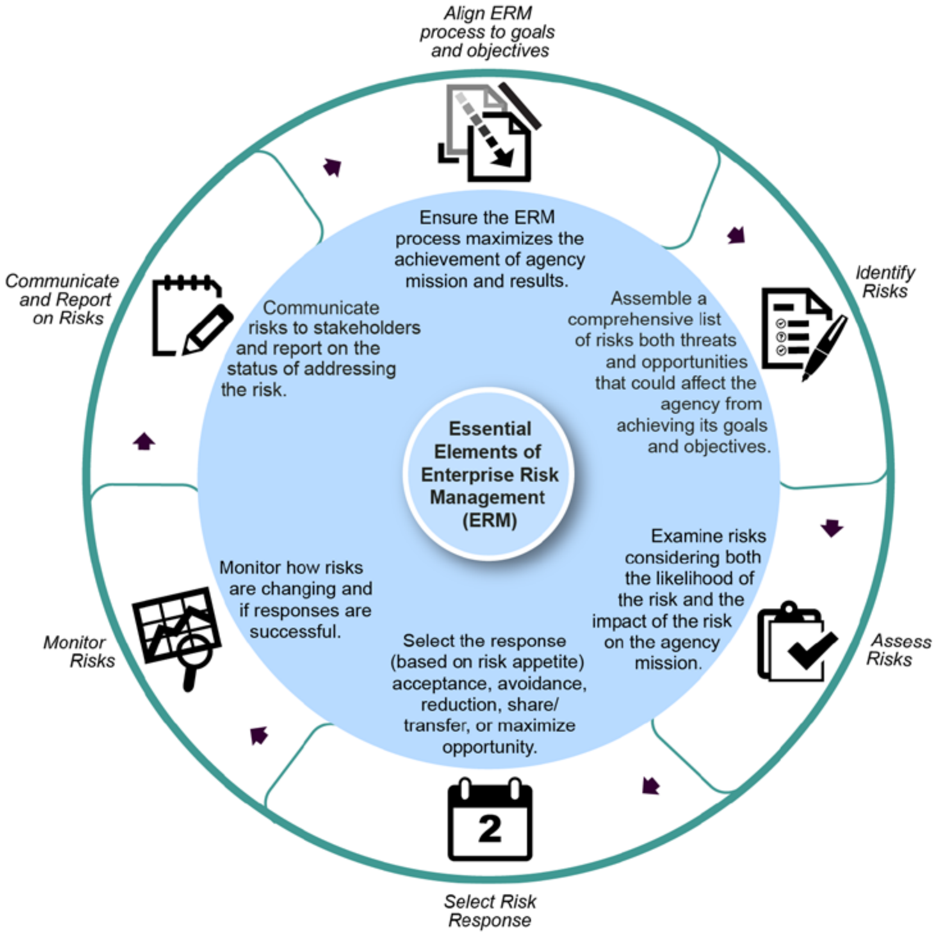
ERM—identifying, assessing, and managing risks—is one component of a governance framework. Organizations develop plans for implementing ERM into management practices that include a planned risk governance structure, processes for considering risk appetite and tolerance levels, a methodology for developing a risk profile, a general implementation timeline, and a general plan for improving the quality of the risk profile and making it more comprehensive over time.

Government, industry, global leaders, and academic institutions have worked together over the last 10 years to develop risk management guidelines that address the unprecedented rate of change in market expectations, global competition, volatile infrastructures, rapidly changing mega trends, and more complex dynamic environments. Published ERM guidelines provide common approaches that can be tailored by industry or business sector. Most warn against practicing ERM within project or program silos, The Government Accountability Office (GAO) suggests that the following are essential elements of risk management at the enterprise level[1]:

- Align ERM process to goals and objectives
- Identify risks
- Assess risks
- Select risk response
- Monitor risks
- Communicate and report on risks

These elements are also depicted in Figure 1.

Figure 1: Essential Elements of Federal Government Enterprise Risk Management


Align ERM process to goals and objectives
Ensure the ERM process maximizes the achievement of agency mission and results.
Identify Risks
Assemble a comprehensive list of risks both threats and opportunities that could affect the agency from achieving its goals and objectives.
Assess Risks
Examine risks considering both the likelihood of the risk and the impact of the risk on the agency mission.
Select Risk Response
2
Select the response (based on risk appetite) acceptance, avoidance, reduction, share/ transfer, or maximize opportunity.
Monitor Risks
Monitor how risks are changing and if responses are successful.
Communicate and Report on Risks
Communicate risks to stakeholders and report on the status of addressing the risk.
Essential Elements of Enterprise Risk Management (ERM)

Source: GAO. | GAO-17-63

[1] Government Accountability Office, GAO-17-63, https://www.gao.gov/assets/690/681342.pdf.

The focus of ERM is on all types of risk that affect organizational goals. The ERM process generates an understanding of the top risks that management collectively believes to be the most critical risks to the strategic success of the enterprise. ERM monitors top risks with key risk indicators, provides opportunities for proactive strategic risk management, and emphasizes results-based performance measurement throughout the organization.

Compliance

Federal Government Standards

The Office of Management and Budget (OMB) Circular No. A-123 was updated in 2016 to ensure that agencies integrate risk management and internal control practices and develop an assessment process[2]. The primary requirements of this policy are summarized as:

- Establish a governance structure for ERM;
- Leverage the existing organizational offices or functions that monitor risks;
- Develop a maturity model approach to the adoption of an ERM framework;
- Continuously identify new or emerging risks and changes in existing risks; and
- Assess the effectiveness of internal controls annually.

Most organizational risk management solutions incorporate the concepts and principles from one of the most widely accepted risk management references by the International Organization for Standardization (ISO): ISO 31000: Risk Management—Guidelines[3]. The ERM principles set forth in this standard are:

- Integrated
- Structured and comprehensive
- Customized
- Inclusive
- Dynamic
- Best available information
- Human and cultural factors
- Continual improvement

The PMA Risk Manager has identified these two standards as the most relevant government-wide references that must be included in the assessment.

[2] OMB Circular A-123, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf.

[3] ISO 31000:2018, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en. Note that although only the introductory sections of the standard are publicly available, the Risk Manager has assured your team that is sufficient for the assessment.

Agency-Specific Requirements

PMA has an Agency regulation (PMAR 800-RM) pertaining to ERM. The main requirements include linking risk to strategic goals and performance objectives, ensuring risks are considered during decision-making, documenting risk acceptance for accountability, and coordinating risk management activities throughout the Agency.

An excerpt of the PMAR 800-RM regulation is included in Appendix A.

Additional Resources

The Risk Manager believes that other sources of information on risk management may prove useful to your team. That list of resources is provided in Appendix B.

Staff Interviews

In July 2019, the Risk Management Working Group performed a series of interviews with PMA staff to collect feedback about the ERM program. The interviews were conducted at all stakeholder levels: senior leaders, middle managers, and team members. The Risk Manager compiled the interview notes and has provided your team with the findings listed in Table 1.

Table 1: Findings from PMA Staff Interviews

PMA’s governing documents are readily available
Risk artifacts are hard to locate because there is no formal repository
There is no executive dashboard for risks
Strong senior leader buy-in for ERM
Risk Management Board and Risk Management Working Group meet on a regular basis
Risk Management Plan is still in draft form
Staff do not have a clear definition of risk management
Risks are identified but not called risks in day-to-day activities
Risk-related roles and responsibilities are unclear at all levels
Risk Management Working Group seeks participation from all PMA offices
Some formal risk direction is provided from the headquarters level to programs and projects

Most staff at the Program Offices do not bother reporting their program risks to Headquarters
Staff has not received formal risk training in the last 12 months
Some risk trending is being performed
Some root cause analysis is performed at the project level
Most reported risks are aligned to support project execution
Performance measures are in place at the project level
No key risk indicators or triggers have been identified
Some knowledge of the PMA risk profile (i.e., the prioritized list of PMA's most significant risks) has been demonstrated
Risk reporting occurs but is not standardized
There are some risk "champions" throughout the Agency, but most staff do not understand the importance of ERM
Staff would encourage more risk taking; PMA is conservative when taking risks
Risk management process is more mature at the research centers than at the headquarters level
ERM culture is fragile – the risk process is perceived as additional work when conducted outside projects

Appendix A
Excerpt from PMAR 800-RM, Project Management Agency Regulation on Risk Management

Section 1: Purpose

This Project Management Agency Regulation (PMAR) provides the requirements for risk management for the Agency, its programs and projects.

This PMAR establishes requirements applicable to all levels of the Agency's organizational hierarchy. It requires formal processes for risk acceptance and accountability that are clear, transparent, and definitive. This regulation also establishes the roles, responsibilities, and authority to execute the defined requirements Agency-wide. It builds on the principle that program and project requirements should be directly coupled to Agency strategic goals and applies this principle to risk management processes within all Agency organizations at a level of rigor that is commensurate with the stakes and complexity of the decision situation that is being addressed.

The implementation of these requirements leads to a risk management approach that is coherent across the Agency in that (a) it applies to all Agency strategic goals and the objectives and requirements that derive from them, (b) it addresses all sources of risk, both internal and external to PMA, (c) all risks are considered collectively during decision-making, and (d) risk management activities are coordinated horizontally and vertically, across and within programs and projects, to ensure timely identification of cross-cutting risks and balanced management of risks Agency wide.

Section 2: Risk Management Overview

In general, risk is concerned with uncertainty about future outcomes. For the purposes of this PMAR, risk is the potential for shortfalls with respect to achieving explicitly established and stated objectives. As applied to programs and projects, these objectives are translated into performance requirements, which may be related to Agency support for mission execution or related to any one or more of the following domains: Safety; Technical; Cost; and Schedule.

This PMAR addresses the application of risk management processes to all Agency activities directed toward the accomplishment of Agency strategic goals, including: strategic planning and assessment; program and project concept development, formulation, and implementation; management of infrastructure, including physical, human, and information technology resources; and acquisition. This PMAR also adds requirements for a formal process of risk acceptance that assigns accountability for each risk acceptance decision to a single responsible, authoritative individual (e.g., organizational unit manager), rather than to a committee or group of individuals. In addition, institutional risks and the coordination of risk management activities across organizational units are addressed.

Section 3: Roles and Responsibilities

Program Offices are responsible for management of technical and programmatic risks within their domains and are responsible for elevating risks to the Risk Management Board at the Agency level. Research Center Directors are responsible for management of project risks at their respective Centers. The Headquarters Office is responsible for Agency-wide risk management. Program and project managers are responsible for program and project risks within their respective programs and projects.

Risk management at the Agency level addresses risks identified at the Agency level, as well as risk decisions elevated from Program Offices. These may have been elevated for any of several reasons, including:
a. A need for the Agency to allocate additional resources for effective mitigation.
b. Agency-level coordination/integration is needed with other organizations/stakeholders.
c. A finding that a risk identified within a Program Office is, in fact, an Agency-level risk.

At each Research Center, management of risks affecting programs/projects at the Center is done within the Center hierarchy and coordinated with the program/project units as needed. Since the program/project units are affected by risks without being in a position to control them, in the event that those risks threaten accomplishment of program/project unit performance requirements, the program/project units may need to elevate them to the next level within the program/project or Center hierarchies.

Section 4: Risk Management Requirements

The manager of each organizational unit shall:
a. Ensure that the risk management processes are implemented within the unit and that key decisions of the organizational unit are risk-informed.
b. Ensure, during procurement activities, that risks are identified and analyzed in relation to the performance requirements for each offeror to the unit and that risk analysis results are used to inform the source selection.
c. Establish elevation criteria to be applied by organizations reporting to the unit.
d. Ensure that cross-cutting risks and interdependencies between risks are properly identified as cross-cutting and either managed within the unit or elevated.
e. Coordinate the management of cross-cutting risks being managed within the unit with other involved organizational units, e.g., Research Centers, Program Offices, programs, projects.
f. Ensure that dissenting opinions arising during risk management decision making are handled through the dissenting opinion process.
g. Ensure that risk management activities of the organizational unit support, and are consistent with, ongoing internal control activities.
h. Ensure the development of a Risk Management Plan that:
(1) Explicitly scopes all the risk types within the purview of the organizational unit, e.g., for programs/projects, these would be safety, technical, cost, and schedule risks.
(2) Delineates the unit's approach for applying risk management.
(3) Cites the documents that capture the complete set of requirements (within the scope established in (1), above) to be met by the organization, including the top-level safety and technical requirements levied on the organization, derived requirements, process requirements, and commitments (e.g., testing).
(4) Is coordinated with other management plans, such as higher level risk management plans and the Systems Engineering Management Plan (SEMP), when applicable.

(5) Defines categories for likelihood and consequence severity, when risk characterization requires specifying risks in terms of such categories. Determines and documents the protocols for estimation of the likelihood and severity of the consequence components of risks, including uncertainty characterization and quantification.
(6) Documents risk acceptability criteria/thresholds and elevation protocols (the specific conditions under which a risk management decision is elevated through management to the next higher level).
(7) Identifies stakeholders, such as Risk Review Boards, to participate in deliberations regarding the disposition of risks.
(8) Establishes risk communication protocols between management levels, including the frequency and content of reporting, as well as identification of entities that will receive risk tracking data from the unit's risk management activity.
(9) Establishes a form for documentation of the manager's decisions to accept risks to safety or mission success, the technical basis supporting those decisions, the concurrence of the cognizant Technical Authorities, and consent of the Risk Takers (if applicable).
(10) Establishes an interval for the periodic review of the assumptions on which risk acceptance decisions are based.
(11) Delineates the processes for coordination of risk management activities and sharing of risk information with other affected organizational units.
i. Ensure that risk documentation is maintained under formal configuration control, with a capability to identify and readily retrieve the current and all archived versions of risk information and the Risk Management Plan.

Appendix B
Additional Sources of Information on Risk Management

National Institute of Standards and Technology (NIST) Risk Management Framework, https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview

Risk and Insurance Management Society (RIMS), https://www.rims.org/

Association for Federal Enterprise Risk Management (AFERM), https://www.aferm.org/

Casualty Actuarial Society (CAS), https://www.casact.org/

Committee on National Security Systems (CNSS), https://www.cnss.gov/cnss/