SMG 2190.1

FDA Staff Manual Guides, Volume III – General Administration

Enterprise Risk Management

FDA Enterprise Risk Management Policy

Effective Date: September 13, 2022
Changed: October 17, 2022

1. Purpose.

The purpose of this document is to formalize the U.S. Food and Drug Administration's (FDA) enterprise risk management (ERM) practices and to provide the policy, roles, and responsibilities for managing enterprise risks in coordination with strategic planning, budgeting, performance management and evaluation, and internal controls functions.

2. Authority.

This Staff Manual Guide (SMG) incorporates guidance and requirements as established in the Office of Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* and OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget.*

The SMG is and will remain aligned with the following FDA policies and processes:

- FDA ERM Council (ERMC) Charter
- Staff Manual Guide (SMG) 2350.1 Guidance for the Implementation of the Federal Manager's Financial Integrity Act (FMFIA)

3. Scope.

This SMG will maintain alignment with the U.S. Department of Health and Human Services' (HHS) ERM Policy and applies to all personnel and offices within FDA. All FDA employees are responsible for adhering to the principles of this ERM SMG and supporting a culture of risk transparency, disclosure, and open dialogue. FDA expects timely and relevant discussions regarding risks.

All ERM functions operating within FDA Centers and Offices shall remain in alignment with this SMG. This alignment will ensure that risks are managed at the appropriate level within FDA and are identified and assessed with consistent methodology and criteria.

4. Policy

The nation's public health relies on the FDA to ensure the safety, efficacy, and security of human and veterinary drugs, biological products, medical devices, our nation's food supply, cosmetics, and products that emit radiation. FDA also has responsibility for regulating the manufacturing, marketing, and distribution of tobacco products to protect the public health and to reduce tobacco use by minors. FDA additionally seeks to improve the effectiveness, safety, and accessibility of medical products and by; and by helping the public get accurate, science-based information they need to use medical products and food to maintain and improve health. FDA also plays a significant role in the Nation's counterterrorism capability. FDA fulfills this responsibility by ensuring the security of the food supply and by fostering development of medical products to respond to deliberate and naturally emerging public health threats.

Existing and potential new risks to FDA's mission continue to require an approach that enables enterprise-wide risk management. FDA maintains an integrated ERM Program that underpins FDA's overall ability to manage risk effectively and efficiently across the Agency.

FDA ERM Program goals are to:

- Effectively identify/anticipate, and respond to enterprise risks, as well as to support more informed management decision-making at FDA.

- Strengthen and maintain appropriate alignment of ERM with the FDA's mission, goals, and objectives, and key management areas such as budget formulation, strategic planning, and performance management.

- Support a risk-informed culture through meaningful engagement on ERM by every Center, Office, and Program that is of clear value to the FDA's understanding of the complex risks and opportunities we face and is integrated with program management and operations.

- Deliver value in providing leaders with a robust and enterprise-wide view of risks to better inform strategic decision-making.

5. Organizational Structure.

FDA's Agency-wide administration of the ERM Program function and responsibilities sits organizationally within FDA's Office of the Commissioner; Office of Operations; Office of Finance, Budget, Acquisition, and Planning (OFBAP); Office of Planning, Evaluation, and Risk Management (OPERM); Division of Enterprise Risk Management (DERM).

6. Roles and Responsibilities.

A. Responsible Parties

1. **FDA Commissioner:** Maintains ultimate accountability for the management of FDA's portfolio of risks across the enterprise, including issuing directives for their management. The Commissioner authorizes and owns the FDA ERM SMG and issues final approval of ERM risk appetite statements. When necessary, makes decisions on prioritizing management of, and funding for, enterprise risks, including as recommended by the Enterprise Risk Management Council (ERMC) and/or Executive Committee (see also 2A and 2B).

2. **FDA Chief Risk Officer (CRO):** The FDA Chief Operating Officer (COO)/Deputy Commissioner for Operations assumes the duties of the CRO and is responsible for the oversight of the ERM Program at FDA, with consultation from the Chief Financial Officer (CFO), OPERM Director, and DERM Division Director. The CRO serves as the principal advisor to the Commissioner, Deputy Commissioners, and Center Directors on all risk matters that could impact FDA's ability to perform its mission.

3. **FDA OPERM Director:** The OPERM Director serves as a principal advisor to the CRO, CFO, and DERM Director on ERM, and is responsible for advising ERM stakeholders and facilitating collaboration across Center/Office leadership, as appropriate.

4. **FDA DERM Director:** The DERM Director serves as a senior advisor to the OPERM Director, CFO, CRO, and Enterprise Risk Management Council (ERMC) and is delegated the responsibility of designing, developing, and implementing the ERM Program at FDA. In day-to-day ERM program practice and management, the DERM Director executes several duties of the CRO, in consultation with the OPERM Director, CFO, and COO as appropriate.

5. **Division of Enterprise Risk Management (DERM):** The DERM Division is responsible for overseeing and managing the implementation of FDA's ERM Program, including the processes for identifying, assessing, prioritizing, mitigating, monitoring, and reporting on key risks. DERM provides advice, guidance, facilitation, and analysis support services on risks that could impair the agency's ability to achieve its mission or goals. DERM also provides all overall agency-wide guidance and training on ERM to which subordinate Center- or Office-level programs must ensure alignment.

6. **Risk Owners** (also known as Leads): Risk Owners are senior executives and senior staff who serve as the FDA's accountable parties who manage an enterprise risk(s).

    a. Oversee the development, implementation, and reporting on the risk responses for the enterprise risk(s), including working with internal partners and subject matter experts to ensure the risk response plan in place sufficiently manages the risk exposure. This includes developing and utilizing appropriate metrics to measure risk progress.

    b. Update, monitor, elevate, or close the risk, informed by qualitative and quantitative analyses and metrics, including Key Risk Indicators, that inform risk response and provide sufficient evidence on the management of the risk.

    c. Report status and any significant changes to the ERMC and the DERM, including periodic reporting and presentations to the ERMC.

    d. Surface progress and challenges related to managing their assigned risk(s) within one's Center/Office and for cross-cutting risks, with Centers/Offices that have roles in supporting management of the response to the risk.

    e. Promote the value of ERM and effectively communicate ERM's alignment with FDA's mission and core functions.

    f. Provide visibility into emerging strategic trends and uncertainties related to the risk.

7. **Risk Champions** (also known as Liaisons, Lead Practitioners, or Points of Contact): Risk Champions have responsibilities related to Agency-wide ERM and FMFIA and are vital to managing the intersection of sound ERM and internal controls programs within their organizations.

    a. Lead the ERM function within their Center or Office and provide overall management and facilitation of their organization's risk portfolio.

b. Maintain accountability for the management of enterprise and Center/Office-level risks, including the implementation and monitoring of response plans and actions.

c. Serve as the main point of contact for requests associated with the risk (includes risk response, action plans, remediation dates), regularly coordinating with the DERM.

d. Confirm reporting is performed on risks and provide periodic updates on Key Risk Indicators (KRIs) to the DERM.

8. **FDA Center and Office Leaders:** Center and Office Leaders are senior executives and senior staff who oversee or lead the execution of programmatic and support functions in FDA Centers/Offices. This includes Executive Officers, Risk Owners, and other Senior Executives and senior staff.

   a. Support implementation of ERM capabilities internal to and across Center/Offices, at various organizational levels, and promote adherence to program requirements.

   b. Actively participate in the development, review, and management of ERM risks housed in one's Center/Office (e.g. enterprise risks on the FDA Risk Profile, FMFIA risks, and other risks on one's Center/Office register).

   c. Provide DERM with organizational points of contact to assist in risk identification, escalation, management, and collaboration, as needed.

9. **FDA Center and Office Employees:** This includes all FDA personnel, and is often referred to as the broader FDA community.

   a. Participate and engage in the ERM process in alignment with ERM program guidance.

   b. Identify and escalate key risks and issues to the appropriate leader in a prompt, and operationally appropriate manner.

   c. Support development, execution, and monitoring of risk responses in one's area.

   d. Provide data, reports, and progress updates on activities to manage FMFIA and ERM to leadership, as appropriate.

   e. Understand the risks that relate to their respective job functions and how the management of risks relates to the achievement of the FDA's

strategic goals and priorities.

B. Governance Bodies

1. **FDA Executive Committee:** The Executive Committee (EC) is FDA's senior governance body and makes strategic, programmatic, and operational decisions for FDA. It is composed of the Commissioner, Chief of Staff, Deputy Commissioners, and Center/Office Directors. The ERMC Chair/Co-Chair periodically briefs the EC on ERM matters and brings recommendations and proposed decisions forward as needed.

2. **The ERMC:** The ERMC bears executive responsibility for governing over Agency-wide risk management at FDA. The ERMC's Charter is included in Appendix 1. The ERMC is composed of executive voting members and non- voting members representing FDA's Centers and Offices.

   ERMC Leadership: Chair, Co-Chair, and Executive Pro-Tempore

   a. Chair: The COO/Deputy Commissioner for Operations serves as permanent ERMC Chair, as Office of Operations' representative to the ERMC, as FDA's CRO, and as FDA's representative on the HHS Enterprise Risk Management Council.

   b. Co-Chair: A Center Director serves as the Co-Chair on a rotating basis.

   c. Executive Pro-Tempore: In the absence of the Chair and Co-Chair, the Chief Financial Officer (CFO) serves as the Executive Pro Tempore and assumes the responsibilities of the Chair and Co-Chair. The CFO also directly ensures that ERMC Leadership guidance is acted upon by OPERM/DERM.

   Responsibilities

   a. Submit Council recommendations to the Executive Committee or Commissioner, including escalation of critical concerns and recommendations for prioritization of risk management responses for specific risks and/or funding as related to those risks.

   b. Establish areas of priority for Council consideration, in alignment with the FDA budget cycle and Strategic Priorities.

   c. Direct the appropriate individuals and teams to implement decisions/actions agreed upon by the Council.

d. Oversee implementation of Council-approved decisions and recommendations.

e. Bring new risks to the Council's attention.

f. Annually submit the FDA Risk Profile to the Agency head.

Center and Office Member Responsibilities

a. Serve as a governing body providing oversight of ERM practice at FDA.

b. Serve as a representative for his/her Center or Office.

c. Consider, approve, and finalize the annual Agency Risk Profile.

d. Make considerations and recommendations to inform and complement decisions across program areas and business operations as related to Agency risks. Includes promoting resourcing of enterprise risks, as appropriate, that are owned by their respective Center or Office by working with budget representatives and Owners to ensure provision of risk related information and data supporting justifications.

e. Monitor emerging and continuing enterprise risks and provide advice on their management to Risk Owners, including on risk response plans and implementation, and monitoring tools such as briefings, key risk indicators, risk appetite, and risk tolerance approaches.

f. Sponsor workgroups for enterprise risks and resolve questions regarding selection of Risk Owners and contributors from their respective organizations to cross-cutting risk management and coordination needs, as necessary.

g. Formalize FDA risk appetite and tolerance statements and determine the Agency's capacity to bear risk.

h. Actively support the integration of ERM with Agency-wide processes, such as strategic planning, budget formulation, performance management, and internal controls.

i. Provide guidance on ERM Program activities within one's Center or Office and advance a risk-informed culture at FDA.

DERM Responsibilities

a. Manage the Agency Risk Profile cycle, including advising Risk Owners and Practitioners in reporting on risks to the Council; bringing new proposed risks to the Council's attention; and ensuring appropriate ERM alignment with budget, strategic planning, performance, evaluation, internal controls, and other related activities for Council consideration.

b. Support and guide Risk Owners and Practitioners on managing and reporting on their risks to the Council.

c. Develop and compile all materials for Council meetings and proposing agendas.

d. Facilitate follow through on decisions, actions, and recommendations agreed upon by the Council.

7. Procedures.

For details on key FDA ERM Program procedures, see Appendix 2.

8. Definitions.

For a glossary of common risk terminology, see Appendix 3 – Relevant Definitions

9. Effective Date.

The effective date of this SMG is September 13, 2022.

10. Document History – SMG 2190.1, "FDA Enterprise Risk Management Policy"

Status (I, R, C)	Date Approved	Location of Change History	Contact	Approving Official
Initial	09/08/2022	N/A	OO/OFBAP/ OPERM/DERM	Jim Sigg, FDA Chief Operating Officer
Change	10/17/2022	Sect. 4; Sect. 6; Appendix 2	OO/OFBAP/ OPERM/DERM	Sarah Lynch, Director, DERM

Back to General Administration, Volume III (2000-3999)

Appendix 1 – ERMC Charter

Please click here for the most recent **ERMC Charter**.

Appendix 2 – Key Procedures

I. ERMC Meetings

A. The ERMC bears executive responsibility for presiding over Agency- wide enterprise risk management and is the decisional body that oversees ERM at FDA.

B. The ERMC generally meets on a quarterly basis, with ad hoc meetings as necessary. Meetings are deliberative in nature.

C. In the first quarter of each calendar year, the ERMC prioritizes FDA's Risk Profile.

D. For other meetings, the ERMC covers governance, response, monitoring, integration, and other key ERM topics to provide guidance, concurrence, recommendations, or decision-making to DERM, the overall FDA ERM Program, Risk Owners, the Executive Committee, and the Commissioner.

II. Risk Profile Process

A. Approving the Annual Risk Profile

1. During the first quarter of each calendar year, the ERMC meets to re-prioritize and approve the FDA Risk Profile.

2. Before the meeting, Council members are given preparatory materials.

3. During this meeting, Council members vote on the following:

    a. Whether any current risks should be removed, escalated, or deescalated

    b. Major changes in scope to existing risks, i.e. risk statements

    c. The addition of any new risks to the profile

d. The final FDA Risk Profile for that calendar year.

4. In consultation with DERM and/or senior leader recommendation, the ERMC may agree to consider addition of compelling new risks, or significantly change the scope of current risks before the annual meeting, if a risk arises for which immediate attention is required. Otherwise, it is expected that responsible Center/Office parties alert and coordinate with the DERM on these updates for the annual Risk Profile review.

B. Developing, Managing, and Updating Risk Response Plans

1. Enterprise Risk Owners develop and/or update Risk Response Plans (Risk Plans) annually, with DERM support and advice as requested. Risk Plans include risk statements, scores, background and root causes, ownership, summary response strategies, and key funding and metrics information related to the management of the risk.

2. Existing Risk Plans can be updated to reflect the management of the enterprise risk throughout the year, as appropriate and including through the FMFIA Process (see III). Updates should be shared with DERM. This includes scope or risk statement, ownership, response strategies (including their effectiveness), and funding gap changes.

3. Enterprise Risk Owners are expected to formally review and update their Risk Plans approximately 6-8 weeks prior to each calendar year (CY) Q1 ERMC meeting; share them with the DERM per deadlines set; and provide information about the response strategies and their effectiveness. This is to ensure that the risk is being actively managed; that additional support can be provided, as possible; and that the ERMC can monitor, at a high level, progress on each enterprise risk's management.

4. For new risks added to the Risk Profile, DERM provides support and advice to the Risk Owner(s) to develop and finalize their Risk Plan(s), as needed.

C. Risk Response Planning and Implementation

1. Following the prioritization of the FDA Risk Profile, DERM coordinates with and advises Top Priority and other Risk Owners to further develop and implement Risk Response Plans for each risk. It is expected that increasingly over time, metrics are included and utilized in risk management approaches.

2. In addition to assisting Risk Owners with response planning, DERM

periodically engages with Risk Owners to provide ERM services to manage and monitor risks.

III. The FMFIA Process and ERM

A. FMFIA/Enterprise Risk Assessment (ERA):

1. As part of remaining compliant with the *Financial Managers' Financial Integrity Act of 1982* and subsequent OMB guidance regarding effective risk management and internal controls, DERM and the Division of Controls Compliance and Oversight (DCCO) coordinate to facilitate annual ERAs in support of FDA's Annual Assurance Statement. ERAs support the evaluation and assertion of effectiveness and efficiency of Centers/Offices internal controls and financial management systems, and the identification and management of risks within Centers and Offices.

2. This process begins late Q1 of each CY, and Center/Offices are required to submit their ERAs during Q2 each CY; it is harmonized with the enterprise risk process and identifies enterprise- and Office/Center-level risks.

3. Following Office/Center ERA submissions, DERM reviews all risks reported with the FDA's CFO and COO. This includes identifying any potential urgent or emerging Center/Office or agency-wide risks and highlighting alignments or changes to enterprise risks.

4. DERM consults with and makes further recommendations to Centers/Offices as appropriate, prior to their submissions of Individual Assurance Statements, and in finalizing ERAs. For more information on this process see SMG 2350.1 Guidance for the Implementation of the *Federal Managers' Financial Integrity Act* (FMFIA).

B. FDA's Risk Register

1. All risks reported to DERM constitute the Agency's annual risk register, which is composed of enterprise risks, FMFIA Center/Office-level risks, and when appropriate, other new or urgent risks that have been identified out-of- cycle.

IV. The Budget Process and ERM

A. DERM and the Office of Budget collaborate closely on all relevant aspects of the annual budget development process, with regular inputs from the ERM Council. Key activities each calendar year include the following:

1. Review and confirmation of enterprise risk funding gaps identified in risk assessment documents (such as Risk Cards) and when appropriate, Center/Office FMFIA Enterprise Risk Assessments.

2. Inclusion and review of risk-informed language to FDA's Budget Justifications.

3. Guidance to the Budget and ERM communities regarding risk- informed Budget processes and associated justifications.

4. Documentation of alignment, and as possible, high-level assessment of proposals for funding support as related to Agency priorities and risks, provided for ERM Council consideration and further recommendation.

5. Consultation with Centers and Offices on new proposals or alignments, as appropriate.

6. Monitoring of the use of funds over time to mitigate identified risks.

B. DERM and the Office of Budget coordinate on major Supplemental investments regarding how they support risk management for new or identified risks, as appropriate.

V. Strategic Priorities and ERM

A. In addition to annual priorities identified on which DERM and the Office of Budget coordinate, the OPERM Director, with support from the DERM Director, provides inputs and guidance regarding risks whose opportunities or mitigations represent or support strategies to advance FDA Strategic Priorities.

Appendix 3 – Relevant Definitions

Enterprise Risk: A risk that has broad or far-reaching implications for an organization as a whole and includes risk to its major programs, operations, reputation, strategy, and reputation.

Enterprise Risk Management: 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 within a single organization/entity. 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.

Internal Control: A process, effected by an organization's management or other personnel, designed to provide reasonable assurance regarding the achievement of objectives.

Issue: An issue is a risk that has occurred or a situation that has arisen that had not been previously identified as a risk.

Risk: The effect of uncertainty on the achievement of objectives.

Risk Appetite: The articulation of the amount of risk (on a broad/macro level) an organization is willing to accept in pursuit of strategic objectives and value to the enterprise. By determining the organization's risk appetite, leadership can determine how much risk they are willing to take when investing in new programs and technologies.

Risk Assessment: The identification and analysis of risks to the achievement of business objectives. It forms a basis for determining how risks should be managed. Risk assessment involves evaluating the impact and likelihood of a risk, as well as any controls or other measures that mitigate or eliminate that risk.

Risk Culture: Risk culture encompasses the general awareness, attitudes, and behaviors of an organization's employees toward risk and how risk is managed within the organization. Risk culture is a key indicator of how widely an organization's risk management policies and practices have been adopted.

Risk Identification: The purpose of risk identification is to find, recognize and describe risks that might help or prevent an organization from achieving its objectives.

Risk Prioritization: Risk prioritization is the process of ranking a set of risks on a highest-to-lowest scale according to FDA's risk rating criteria.

Risk Profile: A prioritized inventory of the FDA's most significant risks.

Risk Tolerance: The acceptable level of variance in performance relative to the achievement of objectives.