



governmentattic.org

"Rummaging in the government's attic"

Description of document: Equal Employment Opportunity Commission (EEOC)
Enterprise Risk Management Handbook (ERM handbook),
2017 and Enterprise Risk Steering Committee meeting
minutes, May-June 2017

Requested date: 23-August-2017

Release date: 17-September-2017

Posted date: 15-April-2019

Source of document: FOIA Request
Assistant Legal Counsel
Equal Employment Opportunity Commission
Office of Legal Counsel
FOIA Programs
131 M Street, NE, Suite 5NW22B
Washington, D.C. 20507
Fax: (202) 653-6034
Email: foia@eoc.gov
[EEOC FOIA Public Access Website](#)

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION
Office of Legal Counsel

131 M St, N. E., Fifth Floor
Washington, D. C. 20507
Toll Free: (877)-869-1802
TTY (202) 663-7026
FAX (202) 653-6034
Website: www.eeoc.gov

September 17, 2017

Re: FOIA No.: 820-2017-003033 (Enterprise Risk Management)

Your Freedom of Information Act (FOIA) request, received on August 23, 2017, is processed. Our search began on August 29, 2017. All agency records in creation as of September 6, 2017 are within the scope of EEOC's search for responsive records. The paragraph(s) checked below apply.

- ☐ Your request is granted.
- ☐ Your request is denied pursuant to the subsections of the FOIA indicated at the end of this letter. An attachment to this letter explains the use of these exemptions in more detail.
- ☐ Your request is procedurally denied as ☐ it does not reasonably describe the records you wish disclosed, or ☒ **no records fitting the description of the records you seek disclosed exist or could be located after a thorough search**, or ☐ the responsive records are already publically available. See the Comments page for further explanation.
- ☒ Your request is granted in part and denied in part. An attachment to this letter explains in more detail.
- ☐ Your request is closed for administrative reasons. An attachment to this letter further explains this closure.
- ☐ A fee of \$ 0.00 is charged. Charges for manual search and review services are assessed according to the personnel category of the person conducting the search a. Fees for search services range from \$5.00 per quarter hour to \$20.00 per quarter hour. Direct cost is charged for computer search and in certain other circumstances. Photocopying is .15 per page. 29 C.F.R. §1610.15. The attached Comments page further explains the direct costs assessed. The fee(s) charged is computed as follows:
- ☐ Commercial use request: ☐ pages of photocopying; ☐ quarter hour(s) of ☐ review time; and ☐ quarter hour(s) of ☐ search time. Direct costs are billed in the amount of ☐ for ☐.
- ☐ Educational or noncommercial scientific institution or a representative of the news media request: ☐ pages of photocopying. The first 100 pages are provided free of charge; and

Re: FOIA No.: 820-2017-003033

☐ All other requests: ☐ pages of photocopying and ☐ quarter hour(s) of search time. Direct costs are billed in the amount of ☐ for ☐. The first 100 pages and the first two hours of search time are provided free of charge.

☐ Please submit payment of \$ 0.00 by either:

(1) Credit card at pay.gov. Visa, MasterCard, American Express and Discover credit cards are accepted. Debit cards bearing the Visa or MasterCard logo are also accepted. We will finish processing your request after EEOC receives a copy of your pay.gov credit or debit card receipt or

(2) Check, payable to the United States Treasurer, to the address above.

☐ The disclosed records are enclosed. No fee is charged because the cost of collecting and processing the chargeable fee equals or exceeds the amount of the fee. 29 C.F.R. § 1610.15(d).

☐ The disclosed records are enclosed. Photocopying and search fees have been waived pursuant to 29 C.F.R. § 1610.14.

☐ I trust that the furnished information fully satisfies your request. If you need any further assistance or would like to discuss any aspect of your request please do not hesitate to contact the FOIA Professional who processed your request or our FOIA Public Liaison (see contact information in above letterhead or under signature line).

☒ You may contact the EEOC FOIA Public Liaison for further assistance or to discuss any aspect of your request. In addition, you may contact the Office of Government Information Services (OGIS) to inquire about the FOIA mediation services they offer.

The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, email at ogis@nara.gov; telephone at (202) 741-5770; toll free 1-877-684-6448; or facsimile at (202)741-5769.

The contact information for the FOIA Public Liaison: (see contact information in the above letterhead or under signature line).

☒ If you are not satisfied with the response to this request, you may administratively appeal in writing. Your appeal must be postmarked or electronically transmitted in 90 days from receipt of this letter to the Office of Legal Counsel, FOIA Programs, Equal Employment Opportunity Commission, 131 M Street, NE, 5NW02E, Washington, D.C. 20507, or by fax to (202) 653-6034, or by email to FOIA@eeoc.gov. <https://publicportalfoiapaal.eeoc.gov/palMain.aspx>. Your appeal will be governed by 29 C.F.R. § 1610.11.

Re: FOIA No.: 820-2017-003033

[X] See the attached Comments page for further information.

Sincerely,

/s/**Sdgarner**

Stephanie D. Garner
Assistant Legal Counsel
(202) 663-4634
FOIA@eeoc.gov

Comments

This is in response to your Freedom of Information Act (FOIA) request. You request the following records:

1. A digital/electronic copy of the ERM handbook (Enterprise Risk Management Handbook), dated approximately April 2017. Your request is granted. A total of 53 pages have been provided for your review.
2. A digital/electronic copy of the meeting minutes for the Enterprise Risk Steering Committee during Calendar Year 2017 to date. Your request is granted. Meeting minutes dated May 24, 2017 (3 pages) and June 5, 2017 (2 pages) have been released for your review.
3. A digital/electronic copy of the EEOC Risk Management Plan. Your request is denied. The plan is currently pending and has not been completed.

This response was prepared by Tracy L. Smalls, Government Information Specialist, who may be reached at 202-663-4331.

EEOC	<i>DIRECTIVES TRANSMITTAL</i>	Number
		195.002
		Date
		04-07-2017

SUBJECT: EEOC ENTERPRISE RISK MANAGEMENT POLICY HANDBOOK

PURPOSE: To establish formal Enterprise Risk Management (ERM) within EEOC in accordance with Section II of OMB Circular A-123 which defines management's responsibilities for ERM and includes requirements for identifying and managing risks, Section 270 of OMB Circular A-11 which discusses agency responsibilities for identifying and managing strategic and programmatic risk as part of the agency strategic planning, performance management, and performance reporting requirements, both of which provide the framework behind OMB Memorandum M-16-17. These constitute the core of the ERM policy framework for the Federal Government with specific ERM activities integrated and operationalized by Federal agencies.

This handbook explains the ERM process and provides actionable steps necessary for a mature and successful ERM program, and provides a path to achieve mature and sustainable ERM activities and processes over time as the EEOC is able to integrate its successive stages. By consistent use of ERM across the organization, EEOC will be positioned to identify and assess risks within the current environment through a systematic process which evaluates the impact of risk on EEOC's ability to more actively achieve its mission and objectives within the limited resources available.

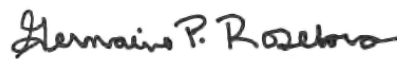
EFFECTIVE DATE: 04-07-2017

DISTRIBUTION:

CURRENT CHANGES: None.

**OBSOLETE DATA
AND FILING**

INSTRUCTIONS: Not applicable. This is a new EEOC Order.



Germaine P. Roseboro
Chief Financial Officer

EEOC	<i>DIRECTIVES TRANSMITTAL</i>	Number 195.002
		Date 04-07-2017

Equal Employment Opportunity Commission



Enterprise Risk Management (ERM)

Policy Handbook

Contents

Abbreviations	4
I. Introduction and OMB Guidance.....	5
II. Integrating ERM and OMB Guidance.....	7
III. Purpose – EEOC Implementation	8
IV. EEOC ERM Objective	8
V. EEOC ERM Roles and Responsibilities	9
1. EEOC Chair	9
2. Chief Risk Officer (CRO)	10
3. Enterprise Risk Steering Committee (ERSC) Representatives	10
4. Office Directors.....	10
5. Management Committees.....	11
6. ERM Team.....	11
7. Program Office ERM Liaisons.....	11
8. EEOC Managers and Staff	11
9. Integrated Project Team (IPT)	11
10. Policy Review and Administration	12
11. Related Laws, Regulations, and Policy Exceptions	12
VI. ERM Process Framework	12
Appendix 1: Guide to the EEOC ERM Framework	15
A. PROCESS DESCRIPTION TERMS	15
B. GUIDE TO PROCESS IMPLEMENTATION	16
Step 1 - Establish the Context Overview	16
Step 2 - Identify Risks	18
Step 3 - Analyze and Evaluate Risks.....	20
Step 4 - Develop Alternatives.....	22
Step 5 - Respond to Risks.....	24
Step 6 - Monitor and Review.....	28
Step 7 – Communicate and Learn (Continuous Risk Identification and Assessment)	30
Appendix 2: Risk Assessment Scales (<i>Pending review by ERSC</i>)	32
Appendix 3: Initial SAMPLE Risk Monitoring and Reporting Templates	36
A. Report 1: SAMPLE Simplified (No Risk Score) Risk Register *	36
B. Report 2: SAMPLE ERSC Top 10 Risk Snapshot Report*	36
C. Report 3: SAMPLE Risk Profile Report*	37
Appendix 4: ERM Lexicon.....	38
Appendix 5: Proposed ERM Risk Taxonomy.....	41
A. General Taxonomy.....	41

B. Taxonomy Risk Area and Risk Category Descriptions	42
Appendix 6: Charter and Implementation Documentation	45

Abbreviations

The following abbreviations are used throughout the document for conciseness:

CMM - Capability Maturity Model
CRO - Chief Risk Officer
EEOC - Equal Employment Opportunity Commission
ERM - Enterprise Risk Management
ERSC – Enterprise Risk Steering Committee
ERMWG - Enterprise Risk Management Working Group
GPRAMA - Government Performance and Results Modernization Act
HSE - Health, Safety, and Environment
IPT - Integrated Project Team
KPI - Key Performance Indicators
KRI - Key Risk Indicators
PAR - Performance Accountability Report
RMC - Risk Management Committee

I. Introduction and OMB Guidance

Enterprise Risk Management (ERM) and Internal Control are components of a robust governance framework. ERM as a discipline deals with identifying, assessing, and managing risks. Through adequate risk management, agencies can concentrate efforts towards key points of failure and reduce or eliminate the potential for disruptive events. Internal control is a process affected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved. As noted in OMB Memorandum M-16-17, ERM will enhance existing communication channels, along with internal controls and governance, which can be visualized as shown in Figure 1.

Figure 1: Relationship between Internal Controls and Enterprise Risk Management



Additionally, M-16-17 goes on to set the framework for Agency implementation with the following guidance:

There are several Enterprise Risk Management (ERM) models available to help organizations integrate risk management and internal control activities into a common framework. Section 270.24 of the Office of Management and Budget (OMB) Circular No. A-11 defines “risk” as the effect of uncertainty on objectives. Risk management is a series of coordinated activities to direct and control challenges or threats to achieving an organization’s goals and objectives. ERM is an effective Agency-wide approach to addressing the full spectrum of the organization’s external and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos. ERM provides an enterprise-wide, strategically-aligned portfolio view of organizational challenges that provides better insight about how to most effectively prioritize resource allocations to ensure successful mission delivery. While agencies cannot respond to all risks related to achieving strategic objectives and performance goals, they must identify, measure, and assess risks related to mission delivery. Effective risk management:

- *creates and protects value;*
- *is an integral part of all organizational processes;*
- *is part of decision-making;*

- *explicitly addresses uncertainty;*
- *is systematic, structured, and timely;*
- *is based on the best available information;*
- *is tailored and responsive to the evolving risk profile of the Agency;*
- *takes human and cultural factors into account;*
- *is transparent and inclusive;*
- *is dynamic, iterative, and responsive to change; and*
- *facilitates continual improvement of the organization*

ERM reflects forward-looking management decisions and balancing risks and returns so an Agency enhances its value to the taxpayer and increases its ability to achieve its strategic objectives. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) ERM framework also includes the concepts of risk appetite, risk tolerance, and portfolio view:

Risk Appetite: *Is the broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision. It is established by the organization's most senior level leadership and serves as the guidepost to set strategy and select objectives.*

Risk Tolerance: *Is the acceptable level of variance in performance relative to the achievement of objectives. It is generally established at the program, objective or component level. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite.*

A portfolio view of risk: *Provides insight into all areas of organizational exposure to risk (such as reputational, programmatic performance, financial, information technology, acquisitions, human capital, etc.), thus increasing an Agency's chances of experiencing fewer unanticipated outcomes and executing a better assessment of risk associated with changes in the environment.*

ERM is beneficial since it addresses a fundamental organizational issue: the need for information about major risks to flow both up and down the organization and across its organizational structures to improve the quality of decision-making. ERM seeks to open channels of communication so that managers have access to the information they need to make sound decisions. ERM seeks to encompass the range of major risks that threatens agencies' ability to implement their missions, programs, and operations. Most agencies should build their capabilities, first to conduct more effective risk management, then to implement ERM, rating those risks in terms of impact, and finally building internal controls to monitor and assess the risk developments at various time points. To complete this circle of risk management the Agencies must incorporate risk awareness into the agencies' culture and ways of doing business.

To meet these goals, EEOC is developing an Enterprise Risk Management (ERM) capability to provide a structured, disciplined, and consistent approach to risk management that facilitates risk-informed decision making throughout the organization. ERM provides EEOC with a means to align strategy, processes, people, technology, and knowledge for the purpose of evaluating and managing uncertainties in executing our unique mission. A consistent approach to risk management across the organization is essential for EEOC leaders to identify and prioritize strategic risks and to prioritize competing requirements in a very restricted funding environment. ERM enables EEOC to more effectively manage enterprise level risks, and it enables agency leaders to consider the trade-offs between risks, associated costs, and value creation across the organization.

This handbook explains the ERM process and provides actionable steps necessary for a mature and

successful ERM program, and provides a path to achieve mature and sustainable ERM activities and processes over time as the EEOC is able to integrate its successive stages. By consistent use of ERM across the organization, EEOC will be positioned to identify and assess risks within the current environment through a systematic process which evaluates the impact of risk on EEOC's ability to more actively achieve its mission and objectives within the limited resources available.

II. Integrating ERM and OMB Guidance

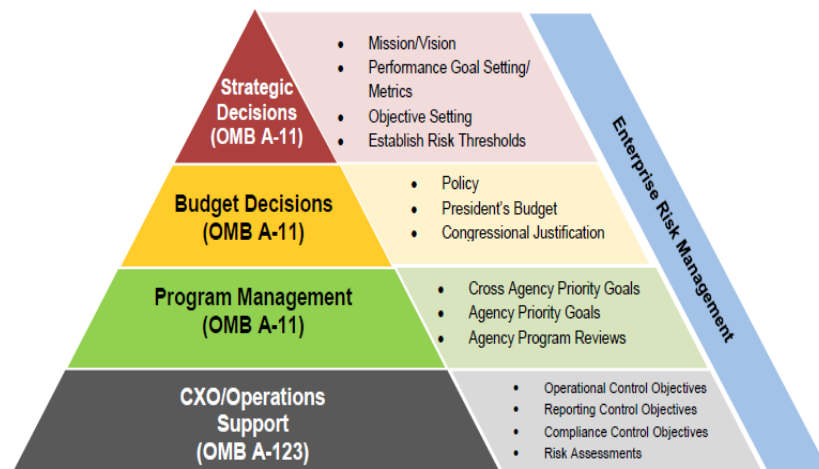
Recent OMB guidance calls for the integration of ERM into existing Government management practices.

Section II of OMB Circular A-123 defines management's responsibilities for ERM and includes requirements for identifying and managing risks. It encourages agencies to establish a governance structure, including a Risk Management Committee (RMC) or similar body; requires the development of "Risk Profiles" to identify major risks arising from mission and mission-support operations; and analyze those risks in relation to achievement of strategic objectives. This complements Section 270 of OMB Circular A-11 which discusses agency responsibilities for identifying and managing strategic and programmatic risk as part of the agency strategic planning, performance management, and performance reporting requirements. Together, these two Circulars constitute the core of the ERM policy framework for the Federal Government with specific ERM activities integrated and operationalized by Federal agencies.

The following figure shows the interplay among OMB Circulars A-123 and A-11 and controls, program management, budget, and strategic decisions within the ERM framework.

As shown in Figure 2, an effective ERM program is an integral part of the agency's strategic decision making process. Agencies should establish risk thresholds and identify top risks to the goals and objectives laid out in their strategic plans. Assessing and prioritizing risks is an important step in operationalizing the strategic plan through the development of program plans, budgets, and the establishment of performance goals and controls.

Figure 2: The ERM Policy Framework



Finally, in September 2014, the Government Accountability Office (GAO) released an updated "Standards for Internal Control in the Federal Government" or "Green Book." This document sets the standards for an effective internal control system for Federal agencies and provides the overall framework for designing,

implementing, and operating an effective internal control system. It included new sections on identifying, assessing, and responding to risks.

III. Purpose – EEOC Implementation

The EEOC's Enterprise Risk Management Handbook (Handbook) serves several purposes. First, the Handbook details the specific duties and responsibilities of EEOC's current and future ERM team, *and* provides information necessary for these individuals to effectively perform their ERM duties.

Second, the Handbook describes the ERM process and provides an overview of the seven-step closed loop process that defines EEOC's framework – from its initial stages to a fully implemented future state. Each process step is described and includes key objectives, “triggers” that affect the successive order of process steps, detail about the corresponding activities, and the roles and responsibilities required of EEOC staff involved in performing the activities. To familiarize those who are new to ERM the Handbook provides them with the context of each ERM process step within the ERM framework to show the inter-relatedness of activities and interactions between EEOC offices.

Finally, the Handbook is intended for use by all EEOC offices to guide the development of our risk management capacity using agency-wide processes and standardized assessment scales. The contents of this document provide the initial blueprint for EEOC's preliminary and ongoing ERM program. Because EEOC is in the initial stages of ERM implementation, some of the appendices are provisional and remain under development. Updates to the Handbook, and all appendices, will occur as development efforts are completed and as the ERM program matures.

IV. EEOC ERM Objective

EEOC's ERM framework provides the means to embed risk management as a core competency in EEOC offices and programs, enabling the agency to fully embed robust and consistent risk management practices at both the enterprise-wide level and within Headquarters Offices, and each Field Office, in a way that facilitates risk-informed decision making at all levels.

The ERM objectives are to:

- Support EEOC leadership through transparency and insight into risks that could impact the ability to execute EEOC's mission through the implementation of well-defined and common risk management processes, tools, and techniques.
- Enable the EEOC to swiftly identify both current and emerging risks and develop plans to respond to risks as well as to take advantage of opportunities.
- Increase the likelihood of success in achieving the objectives of EEOC's mission and Strategic Plan.
- Improve the understanding of interactions and relationships between risks.
- Establish clear accountability and ownership of risk.
- Develop the capacity for continuous monitoring and reporting of risk across the Agency from the operational level to the Executive Risk Steering Committee (ERSC).
- Develop a common language and consistent approach across all EEOC Offices that help to establish the broad scope of risk and to organize risk management activities.
- Build credibility and sustain confidence in EEOC's governance and risk management by all stakeholders including industry, federal, state, and local partners, and the public which we serve.
- Ensure that risks are managed in a manner that maximizes the value EEOC provides to the

workforce, both employer and employee, consistent with a defined risk appetite and risk tolerance levels.

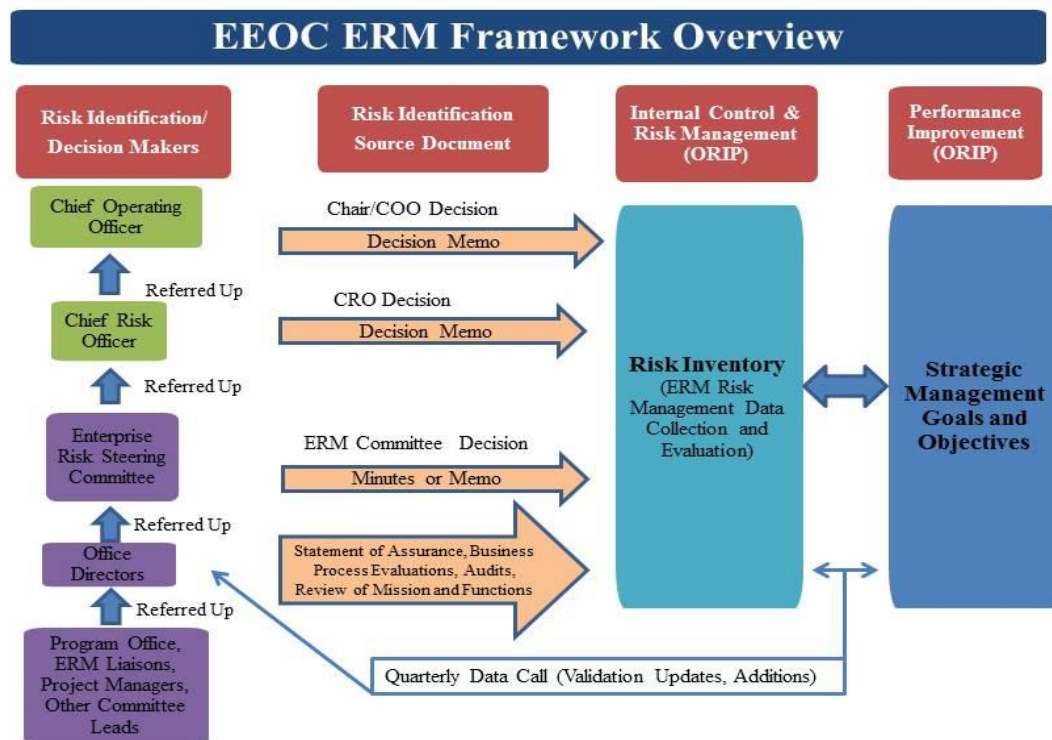
EEOC recognizes that many risks within the organization are interrelated and cannot be effectively and efficiently managed independently within a given Headquarters or Field Office. These interconnected risks facing EEOC must be managed across the organization and, in many instances, in coordination with the agency and its stakeholders. This Handbook sets forth initial guidance and repeatable processes and activities to identify, analyze, evaluate, respond, and to effectively identify and manage the various risks to EEOC's successful mission accomplishment.

V. EEOC ERM Roles and Responsibilities¹

1. EEOC Chair

The EEOC Chair maintains ultimate accountability for the management of the agency's risks, including issuing directives for their management. The Chair also authorizes the EEOC ERM Policy and issues final approval of the ERM risk appetite statements. Figure 3 depicts the Relational Organizational Chart for the management and oversight of the EEOC ERM Program.

Figure 3: Enterprise Risk Management Framework Overview



These activities are described below.

¹¹ All relevant roles are listed in this Handbook and are in accordance with OMB guidance.

2. Chief Risk Officer (CRO)

The CRO serves as the principal advisor to the Chair and the Chief Operating Officer on all risk matters that could impact EEOC's ability to perform its mission. The CRO is responsible for the design, development, and implementation of the ERM program at EEOC. The CRO, in conjunction with the EEOC ERM Team, will lead EEOC in conducting regular enterprise risk assessments of EEOC business processes or programs at least quarterly and will oversee the identification, assessment, prioritization, response, and monitoring of enterprise risks. The CRO will also lead EEOC strategic planning and integration of risk management (RM) principles across the enterprise. The CRO, in collaboration with the EEOC Chief Information Officer, will develop the strategic risk architecture, and align systems and technical architecture efforts across Headquarters and the Field for proper integration.

3. Enterprise Risk Steering Committee (ERSC) Representatives

The ERSC will be composed of the following representatives:

- Chief Risk Officer (CRO) and Committee Chair
- Director, Office of Field Programs
- Director, Office of Federal Operations
- District Director Representative
- Regional Attorney Representative
- Field/ Area/Local Office Director Representative
- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- Director, Office of Research, Information and Planning (ORIP)
- Deputy General Counsel
- Director, Legal Counsel
- Chief Financial Officer (CFO)
- Chief Human Capital Officer (OCHCO)

The ERSC's Chair is the Chief Risk Officer (or designated ERSC Office Director when the CRO is not available) and reports to the Chief Operating Officer. As required, the ERSC oversees the progress of working groups that will consist of executive and staff level participants. Working groups develop detailed plans defining milestones and key deliverables that meet requirements and tasks from the ERSC.

Headquarters Office Directors are permanent ERSC members, and Field representatives will serve two year terms. The Chair will select Field representatives to the ERSC. A term follows the fiscal year cycle.

4. Office Directors

Office Directors, who comprise EEOC's Senior Leadership Team, serve as ultimate risk owners in accordance with the ERSC Charter. All Headquarters and Field Offices will adopt and follow the ERM framework and the EEOC ERM Policy and participate in enterprise-wide risk management efforts and perform risk management activities within their individual office. Office Directors are responsible for implementing consistent risk management practices in alignment with this policy. It will be the responsibility of all Headquarters and Field Offices to break the enterprise level risk appetite statements into Program Office specific risk limits, where applicable.

Headquarters and Field Office Directors will also assist the ERM Team in creating ad-hoc risk analysis teams to serve as Subject Matter Experts (SMEs) during the risk identification and analysis process.

5. Management Committees

Management Committees include EEOC's other decision-making bodies, such as the IT Investment Review Board, the Action Council for the Transformation to Digital Services (Act-Digital), and EEOC Senior Executive Service (SES) members. Executives should ensure that decisions made in these forums are risk-informed and that staff use accepted Agency methodologies for assessing risks.

6. ERM Team

The ERM Team will consist of individuals from the Office of the Chair, Office of the Chief Financial Officer, Office of the Chief Information Officer, and the Office of Research, Information and Planning. The ERM Team leads ERM activities under the supervision of the CRO and ORIP Director. Such activities include developing and maintaining ERM policies, processes, procedures, tools, and information systems; leading efforts to perform enterprise risk identification, assessment, prioritization, reporting, and monitoring; and, establishing ERM communication at all levels and for gathering data and developing risk reports.

7. Program Office ERM Liaisons

Program Office ERM Liaisons are designated individuals within each EEOC Office that serve as the primary representative to the ERM Team. ERM Liaisons share information and provide subject matter expertise to support ERM program activities, such as the identification, validation, and assessments of enterprise risks. This group also serves as the primary point of communication between the ERM Team and its members' respective Office(s). There shall be a core team of advisors on the ERSC and ERM Team which represent each Office, but other EEOC subject matter experts (SMEs) may be identified to participate on an as-needed basis. ERM Liaisons are responsible for communicating with the ERM Team and supporting Office risk owners throughout the ERM process, as necessary.

8. EEOC Managers and Staff

All EEOC managers, staff, and contractors have an important role in identifying and managing risk across the enterprise. They are expected to make and support risk-informed decisions and remain vigilant in spotting and identifying emerging risk issues that could jeopardize EEOC's success. To the extent that any employee or contract staff becomes aware of what appears to be a significant risk-related issue, the employee should notify his or her supervisor or Contracting Officer's Representative, so that action may be taken as appropriate.

9. Integrated Project Team (IPT)

IPTs will be chartered by the ERSC to coordinate and implement, as directed, internal risk management strategies and procedures, or other risk-related efforts. IPTs are comprised of cross-functional subject matter experts (SMEs) that are responsible for assessing a defined risk to identify cross-functional root causes and consequences. IPT members will assist the ERM Team and Risk Owners to develop event trees or scenarios, estimate probabilities and impacts, identify

risk response options, perform cost-benefit analysis, identify Key Risk Indicators (KRIs), and develop recommendations for risk response and monitoring plans.

10. Policy Review and Administration

The content and the level of detail of the ERM policy will evolve as the EEOC ERM program matures. The ERM Team and ERSC will review the EEOC ERM policy every year, at a minimum, and provide recommended changes for consideration and approval by the CRO prior to finalizing any future revisions.

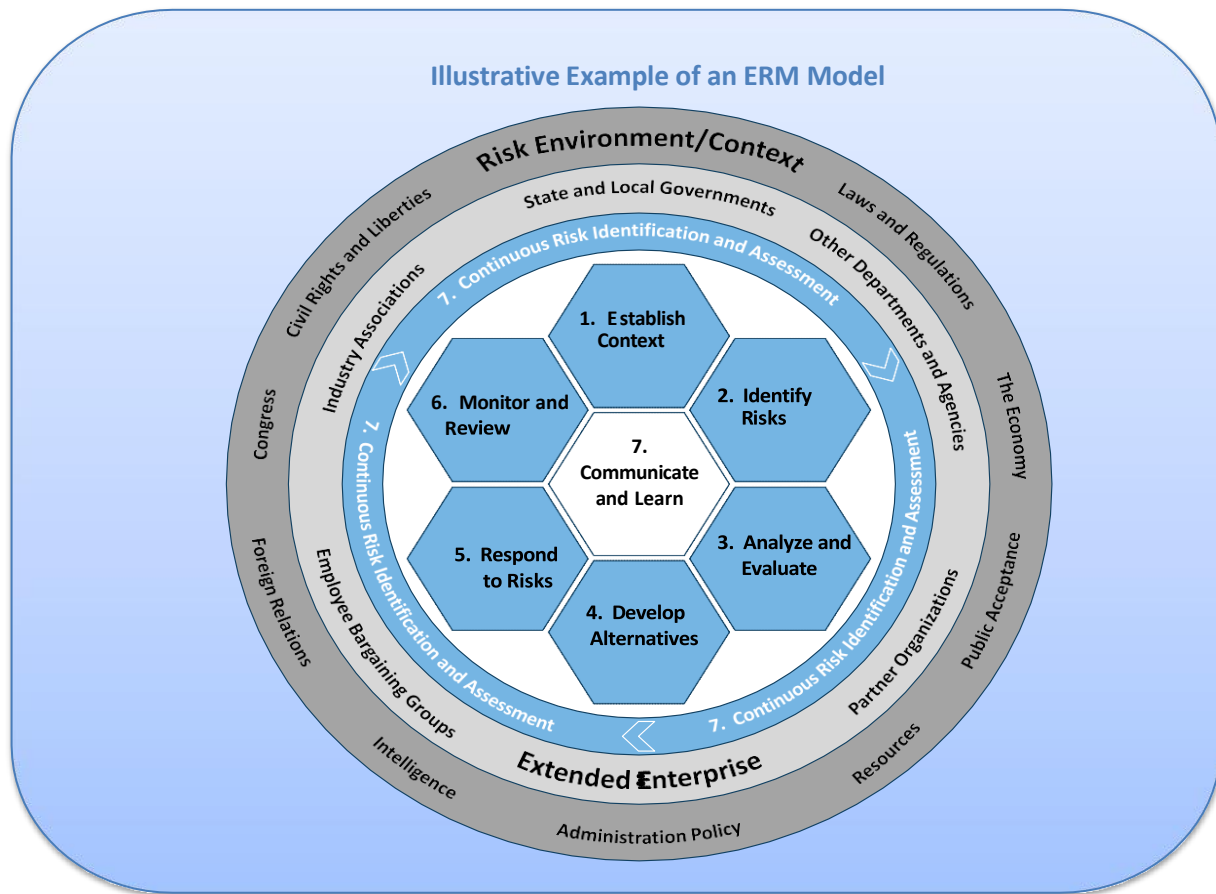
11. Related Laws, Regulations, and Policy Exceptions

ERM policies, procedures, and activities must comply with Government Statutes and Laws as well as requirements dictated by the U.S. Congress, the Office of Management and Budget, U.S. Government Accountability Office (GAO), and other relevant stakeholders. Any exception to this policy must be documented in writing and approved by the Director of the requesting Office and forwarded to the CRO for notification, review, and approval. The ERM Team will track policy exceptions and report this status to the ERSC.

VI. ERM Process Framework

The ERM process framework depicted below in Figure 4, which is presented in the GSA Enterprise Risk Management Playbook, as well as OMB M-16-17, is being implemented by EEOC. It is aligned with the EEOC Strategic Plan.

This risk management process provides a logical and systematic method for establishing the context for risks, as well as identifying, analyzing, evaluating, responding to, monitoring, and communicating them in a way that will allow EEOC to make decisions and respond to risks and opportunities as they arise. This approach promotes comparability and a shared understanding of information and analysis in the decision process and facilitates a better risk management structure and risk-informed decision making.

Figure 4: EEOC Enterprise Risk Management Process

The seven steps can be summarized, and will be elaborated on with detailed plans for implementation in [Appendix 1](#), as follows:

1. **Establish the Context** - understanding and articulating the internal and external environments of the organization.
2. **Initial Risk Identification** - using a structured and systematic approach to recognizing where the potential for undesired outcomes or opportunities can arise.
3. **Analyze and Evaluate Risks** - considering the causes, sources, probability of the risk occurring, the potential positive or negative outcomes, and then prioritizing the results of the analysis.
4. **Develop Alternatives** – for the highest priority risks, systematically identifying and assessing a range of risk response options guided by risk appetite.
5. **Respond to Risks** - making decisions about the best option(s) among a number of alternatives, and then preparing and executing the selected response strategy.
6. **Monitor and Review** - evaluating and monitoring performance to determine whether the implemented risk management options achieved the stated goals and objectives.
7. **Communicate and Learn** - Once ERM is built into the Agency’s culture, it is possible to learn from managed risks, near misses, and adverse events; and those lessons can be used to

improve the process of risk identification and analysis in future iterations. ERM must be an iterative process, occurring throughout the year to include surveillance of leading indicators of future risk from internal and external environments.

This Seven Step process will be integrated into existing Agency planning, performance management, and budget processes.

Appendix 1: Guide to the EEOC ERM Framework

A. PROCESS DESCRIPTION TERMS

To add to the understanding and use of the ERM process, each of the seven steps (Establish Context, Identify Risks, Analyze and Evaluate, Develop Alternatives, Respond to Risks, Monitor and Review and Communicate and Learn) is described using a consistent format with each element described below.

Overview: The Overview section provides a short description of the process describing its key elements. This contains a summary of the process to provide context and orient readers with the content.

Objectives: The Objectives section describes the purpose for performing the process. The objective statement is a high-level statement that explains the ‘why’ but not the ‘how’ of the process inputs being transformed into process outputs.

Triggers: The Triggers section describes what prompts or initiates the process to occur and when, if time dependent. A process must have at least one trigger, but may have many. In some cases the trigger may be a scheduled start date. For example, *Establish the Context* could be scheduled on an annual basis during a particular month. Another typical trigger would be the completion of the preceding process in the risk management framework. For example, *Analyze Risks* is performed upon the completion of *Identify Risks*.

Inputs: The Inputs section lists all materials, data, or information required to perform the process. Inputs can consist of: Output from a preceding or parallel process; publications, notifications, or formal communications; data from a database or other source; and documents or reports providing information or data.

Activities: The Activities section lists and describes each activity. Each activity within the process is a task or set of tasks required to produce the desired outputs from the inputs. Activities are best defined for a single organizational unit to simplify procedure-writing. However, many activities require close interaction among two offices or functions that may be either internal or external to EEOC. These should be evaluated on a case-by-case basis.

Process owner(s): The Process Owners section outlines those individuals with accountability for the outlined activity. These individuals oversee the activity to be performed and have sufficient authority to enforce policies and procedures and authorize the resources to carry out span of activity.

Process participants: The Process Participants section lists the roles of individuals required to perform the activities. However, there may be other process participants, and they will be listed in each section.

Outputs: The Outputs section lists the materials, information, or data produced by the process. Outputs can consist of: Input to another process; publications or formal communications; alerts or notifications; interfaces to another process; data written to a database or other source; documentation or reports providing information or data.

B. GUIDE TO PROCESS IMPLEMENTATION

Step 1 - Establish the Context Overview

The *Establish the Context* process step involves understanding and articulating the internal and external environment of the organization. During this step is where EEOC defines its objectives, evaluates the external and internal parameters to be taken into account when managing risk, makes changes to the risk management process, and develops risk criteria.

Objectives

To establish the scope of the risk management process by reviewing EEOC's strategic objectives, environment, risk management objectives, and the criteria against which risks will be assessed.

Triggers

These are some of the triggers for conducting this step of the process:

- Annual context review performed each **July (TBD)**
- Major changes in organizational structure, such as the formation of a new Office
- Congressional, Administration, or other mandates affecting risk management processes
- Occurrence of a major risk event where "major" refers to risk events having a high degree of severity on the enterprise impact scale

Inputs

- EEOC mission statement, vision, strategic goals, and objectives
- OIG audit reports and findings
- IT System Risk Assessments, Annual Control Reviews, and Plans of Actions and Milestones
- EEOC FMFIA and Performance Accountability Reports
- EEOC Strategic Plan, Strategic Enforcement Plan, and related supporting documents
- EEOC ERM Policy, risk appetite statements, roles and responsibilities, organizational structure charts, and ERSC Charter
- Existing ERM process documentation
- GPRA measures, including the Performance Accountability Report (PAR)
- Information about major changes in external or internal environment affecting strategic objectives or risk profile
- Analysis of risk response options and controls effectiveness
- Scope of risk assessments (from previous year or last time developed)
- Stakeholder analyses and inputs

Process participants

- ERSC
- CRO
- ERM Team
- ERM Liaisons
- Risk Owners

Activities

1. Evaluate external, internal, and risk management context (ERSC, CRO, ERM Team, ERM Liaisons, Risk Owners). Review existing EEOC risk documentation, including the risk lexicon (see inputs above), to assess whether current policies and procedures are sufficient, or if additional criteria and policies should be developed. Review should include changes in EEOC's internal and external environment such as: Newly-identified emerging risks, legal framework volatility, changes to protected bases, etc.
2. Adjust risk assessment criteria, policies, and charters (CRO, ERM Team, and ERM Liaisons). Identify the types of impacts which are most critical to EEOC through interviews with EEOC leadership and ERSC members. Ensure definitions of levels of impacts are relevant to appropriately reflect EEOC's risk appetite and tolerance. Obtain guidance and approval for changes from appropriate parties, including ERSC members.
3. Approve risk criteria, policies, and charters (CRO and ERSC). Review proposed policy, charter, and risk criteria revisions submitted by the ERM Team. Provide comments and feedback to the ERM Team. Communicate development of changes and confirmed revisions to the Senior Leadership Team (SLT) to endorse agreed revisions.
4. Propose risk assessment scope (ERM Team). Determine the scope of risk identification and assessment activities for the year by annual review of the Risk Register. Review any changes to the internal and external risk management context, and identify business activities requiring a re-assessment of risks. Input and guidance should be sought from Risk Owners in defining the scope for the risk assessments. Obtain agreement from Risk Owners as to whether or not risks in their area require re-assessment during the coming year.
5. Define risk assessment scope (Risk Owners). Review anticipated mission and business operations for the coming year and determine if any changes in the external context should trigger a reevaluation of existing risks, or the identification of new and emerging risks. Review proposed risk assessment scope provided by ERM Team and provide input.
6. Approve EEOC risk assessment scope (ERSC). Review the risk assessment scope proposed by ERM Team and reviewed by Risk Owners, provide input and guidance, attend meetings, and vote on the endorsement.
7. Update ERM Risk Register (ERM Team). Review the structure and elements of EEOC's Risk Register and other risk management systems and tools in light of the previous activities. Determine if any changes need to be made, update processes and procedures to reflect the changes, and communicate the changes to affected parties.

Outputs

- Updated ERM Policy, risk appetite statements, roles and responsibilities, organizational structure charts, and ERSC Charter
- Updated impact, likelihood scales, and tolerance thresholds
- Risk assessment scope (for current year)

Step 2 - Identify Risks

Overview

During the *Identify Risks* process step, EEOC seeks to identify enterprise-level risks to be managed using a structured, systematic process called the Enterprise Risk Register. This process specifies what risks can occur, as well as where, when, why, and how they may occur. At this stage in the overall framework, the primary concern is to identify as many risks to achieving the EEOC's mission and vision as possible, the sources of the risks, and the impacts. The list of risks identified through this process is preliminary and subject to further qualification and refinement as part of the following *Analyze Risks* process. The *Identify Risks* process captures risks using EEOC's enterprise risk taxonomy and then progressively narrows the list to the most critical using first qualitative and then quantitative techniques in the *Analyze Risks* process.

Objectives

To identify a comprehensive list of risks and events that may potentially impact the achievement of EEOC's mission and strategic objectives.

Triggers

- Completion of *Establish the Context* process

Process participants

- ERSC
- CRO
- ERM Team
- ERM Liaisons
- Risk Owners

Inputs

- Audit reports and findings
- Stakeholder analyses and inputs
- Updated ERM Policy, risk appetite statements, roles and responsibilities, organizational structure charts, and ERSC Charter
- Updated impact, likelihood scales, and tolerance thresholds (if applicable)
- Processes
- Other information (e.g., Department of Justice)
- GAO reports
- EEOC Risk Map

Activities

1. Research and identify emerging risks (ERM Team and Risk Owners). Perform scenario analysis exercises periodically, and review the major risks associated with existing Key Performance Indicators (KPIs) or other performance metrics associated with achieving mission success. Review the scenario analyses from similar organizations (e.g., other Federal agencies or

- Commissions) if available, as well as private sector EEO counterparts.
2. Review the Risk Register for new, changed, and obsolete risks (ERSC, CRO, ERM Team, ERM Liaisons, and Risk Owners). Review risk taxonomy to identify risk types on which to focus the risk identification and review activities. Risk Owners will perform this process for their office or program level, and the ERM Team will perform this at the Headquarters Office level. Conduct cross-functional meetings to further identify which risks are new, changed, or obsolete in terms of their impact or likelihood.
 3. Identify risk factors and consequences (ERM Team and Risk Owners). Develop preliminary lists of risk factors and consequences. Assist EEOC's ERM Team with identifying the Risk Owner for new risks and confirm the Risk Owner for changed risks. Assist with the identification of staff that will be able to identify and quantify the risk factors and consequences. If the risk is determined to be high enough to be elevated to the EEOC's Risk Register, then this initial list of risk factors and consequences will be used as the starting point for an expert panel to build out event trees.
 4. Map risks to strategic objectives, Key Performance Indicators (KPIs), and processes (ERM Team, ERM Liaisons, Risk Owners). Specify the strategic objective to which the risk applies. Identify and capture the KPIs used to measure the risk. These should be drawn from existing KPIs specified as part of the performance goals. If new KPIs are identified during the risk management process, then these should be communicated to the affected staff for incorporation into process documentation and departmental objectives and performance measures. Specify the risk tolerance for each KPI. The risk tolerance can be expressed as a threshold that is not to be breached or as an acceptable band depending on the particular KPI in question.
 5. Update EEOC's Risk Register (ERM Team). Update the information in EEOC's Risk Register for existing risks. Add new risks and preliminary information to be elaborated and validated during the risk evaluation. Delete obsolete risks and document the reason. Map each risk to the operational activities or processes it resides in.

Outputs

- KPIs and risk tolerance thresholds
- Updated and new mappings to operational activities or processes
- Updated Risk Owners
- Updated EEOC's Enterprise Risk Register

Step 3 - Analyze and Evaluate Risks

Overview

The *Analyze and Evaluate Risks* process involves consideration of the causes and sources of risk, the probability that the risk event will occur, their positive or negative consequences and magnitude, and the likelihood that those consequences may occur. Risk analysis provides the basis for evaluation and decisions regarding risk response or treatment. Each risk identified during the *Identify Risks* process is subjected to a qualitative evaluation of its likelihood and impacts. The list of risks is then narrowed and refined based on the criticality of the risk. Those risks falling below a defined threshold may continue to be monitored and managed within EEOC, but will not be reported at the executive level as part of the Enterprise Risk Register.

After the initial screening using qualitative techniques, a determination will be made regarding how accurate the estimates of likelihood and impact are for prioritizing, measuring, and reporting the risk and to select the appropriate risk response options. Risk assessment techniques range along a spectrum. Qualitative risk assessment techniques use scales representing ranges of likelihood and impact, more quantitative techniques may include what-if scenario analyses using complex quantitative models. Initially, EEOC will rely more heavily on qualitative assessments until quantitative measures are developed and implemented. EEOC's risk assessment tools and techniques will evolve over time, and as the ERM program matures a shift to more quantitative analysis is expected. The assessment scales used to qualitatively assess the risks are contained in Appendix 1.

Objectives

To estimate the magnitude of the likelihood and impact of risks using qualitative and deterministic quantitative methods while laying the foundation for future quantitative risk modeling.

Triggers

- Completion of *Identify Risks*
- Occurrence of a risk event(s)
- The publication of a risk assessment by internal or external stakeholders supporting different conclusions regarding the likelihood or impact of a risk or the effectiveness of existing controls
- To be performed annually or more often if events warrant as specified in the triggers for *Establish the Context*.

Inputs

- Qualitative assessment scales
- Advanced risk modeling testing results, if applicable
- Internal and external audit reports
- Internal and external data and information sources
- Stakeholder input
- Updated EEOC Risk Register

Process Participants

- ERM Team
- ERM Liaisons

- Risk Analysis IPTs
- Risk Owners

Activities

1. Facilitate qualitative assessment and assign risk ratings (ERM Team, Risk Analysis IPTs, and Risk Owners). For risks that have causal links or impacts that affect more than one program or Office, it is likely that the staff best qualified to estimate likelihood and impact will come from multiple Offices. In this case, solicit the assistance of the ERSC members if necessary, to assist with securing resources across EEOC, and build the appropriate reporting relationships.
2. Aggregate and prioritize risks (ERM Team). Assign a rating of severity and likelihood to each risk and record the risk rating in the Risk Register. Assess all risks with risk ratings of high severity and high likelihood at EEOC's level and prioritize the risks for various types of analysis. For visualization purposes, risks may be plotted on a heat map based on the defined impact and likelihood scales for EEOC.
3. Develop or update event trees (Risk Analysis IPTs and Risk Owners). Identify risk analysis IPTs of individuals intimately familiar with the select risk to develop causal chains of events that could lead to the risk. Organize these as "triggering events" that lead to secondary risk factors ultimately leading to the risk event. Identify the chains of impacts resulting from the risk occurrence and link secondary impacts to primary impacts. For existing event trees, reconvene with the appropriate expert staff to identify if the risk factors and impacts shown still apply.
4. Facilitate event tree development and updates (ERM Team). Provide training on how to develop event trees as required. Provide assistance with facilitating expert panel sessions if requested. Review the likelihood and impact data for reasonableness and alert the Risk Owners and Risk Analysis Team of any potential issues. Assist the Risk Owner and Risk Analysis IPT with identifying Key Risk Indicators (KRIs).
5. Quantify selected risks (ERM Team, Risk Owners, and ERM Liaisons). For each causal chain of risk factors in a new event tree, estimate the annual frequency of the trigger event, the probability that the second risk factor will occur if the trigger occurs, and the severity of the loss should the second risk factor occur. For each impact, estimate the probability of occurrence.
6. Develop EEOC's risk portfolio (ERM Team). After all the risk factors and consequences have been quantified, calculate various risk measures to express all risks as an enterprise-wide risk measure such as "percent of budget at risk" or "percent of security effectiveness at risk."

Outputs

- Enterprise-wide risk measures for the EEOC's complete portfolio of risks
- Event trees analysis
- Identified relationships between risks
- KRIs
- Qualitative and quantitative analysis
- Updated EEOC Risk Map and Risk Register

Step 4 - Develop Alternatives

Overview

The *Identify Risks* process uses the qualitative risk analysis generated in the preceding *Analyze and Evaluate Risk* process to rank and prioritize enterprise level risks. The focus of ERM is not to try and identify and analyze every risk facing EEOC, but to identify those risks that rise to the enterprise wide level. By prioritizing the enterprise-level risks, EEOC leadership can respond as appropriate with strategic allocation of resources in the *Respond to Risks* process. Usually, risk managers find that responding to a few critical risks results in dramatic reductions in residual risk. At this stage, EEOC leadership should have more enterprise-wide quantitative information regarding risks from across the organization that may not have been available earlier during the *Establish the Context* or *Identify Risks* processes. During *Develop Alternatives*, EEOC leadership should revisit the documented risk tolerances in light of their overall risk portfolio and make adjustments.

Objectives

To develop a prioritized list of enterprise-level risks for response options/alternatives.

Triggers

- Completion of *Analyze and Evaluate Risks*
- To be performed annually or more often if events warrant (as specified in the triggers for *Establish the Context*)

Process Participants

- ERSC
- ERM Team
- ERM Liaisons
- Risk Analysis IPTs
- Risk Owners

Inputs

- Analysis of risk response and controls effectiveness
- Calculated enterprise-wide risk measures for the EEOC's complete portfolio of risks
- Event trees analysis
- Identified relationships and correlations between risks
- KRIs and KPIs
- Qualitative and quantitative analysis
- Risk tolerance thresholds
- Stakeholder Input
- Updated EEOC Risk Map and Risk Register

Activities

1. Compare risk levels to risk criteria (ERM Team). For each risk factor, risks, and risk consequence identified, compare the calculated risk measures to the risk tolerance thresholds

defined as part of the *Identify Risks* process.

2. Provide input on risk rankings and prioritization (Risk Owners, ERM Team, and ERM Liaisons). Provide any additional required input on qualitative impacts, mission objectives, risk tolerance, or threshold criteria, and any other considerations that would impact the relative ranking and prioritization of risks for response options. Review event trees and risk correlations in order to understand the interrelated nature of risks and how they might impact risk prioritization.
3. Rank and prioritize risks (ERM Team). Prioritize the risks for risk response options. Involve Risk Owners and Program Office Staff responsible for managing the risks. Review event trees and risk correlations to prepare a report on the ranked list of risks and the approach and rationale used to rank the risks and present it to the ERSC for endorsement. Update information about EEOC's risks and enter their rankings in the Enterprise Risk Register.
4. Approve risk prioritization (ERSC). Review the report on the ranked list of risks that will be considered for risk response options. Offer guidance on any pending management decisions, planned projects, changes to strategic direction, or other factors that might impact the ranking of the risks. Request and review changes from the ERM Team. Vote to endorse the ranked list prior to presenting it to the SLT for approval.

Outputs

- Prioritized list of quantified risks requiring response options
- Stakeholder Input
- Updated EEOC Risk Register

Step 5 - Respond to Risks

Overview

The *Respond to Risks* process involves identifying and assessing the range of risk response options and preparing implementation plans for selected response options. Responding to risks includes both the seizing of opportunities to achieve mission success as well as efforts to minimize the adverse impacts of risk. Using a prioritized list of quantified risks requiring response options from the *Evaluate Risks* process, EEOC leadership can make informed strategic decisions about how to allocate resources to programs and projects reflected in the enterprise risk register.

Decision Authority Matrix

Decision Maker	Escalation Criteria	Decision Authority
Chair	Discretion	-Allocate Resources -Approve cross service risk mitigation plans
Chief Operating Officer	Discretion	-Recommend allocation of resources -Recommend cross service risk mitigation plans
Chief Risk Officer	Discretion of Office of the Chair -High political sensitivity -Risk to EEOC core mission -Significant regulatory risk	-Recommend allocation of resources -Recommend terminate or delay project -Delegate risk management authority/ownership -Recommend cross service risk mitigation plans
Enterprise Steering Committee	-Enterprise wide impact -Requires additional resources, funds -Decision required to delay or terminate -Highly political/regulatory compliance risk	-Escalate if needed -Request allocation of resources -Approve mitigation plans for “Non” escalated risks -Risk management authority to Office Director
Office Directors	-Impacts to program/projects -Political sensitivity -Requires Allocation of funds -Expected significant delay in implementation or completion -Cannot be resolved immediately or a matter of days	-Escalate if needed -Approve mitigation plans for “non-escalated risks -Monitor/manage risks that do not require escalation -Delegate risk ownership to program/project/Committee lead. -Ensure risk reviews and plans are sent to ORIP
Program/Project/Committee Leads	-All identified risks go through the risk management process -Approved risks are prioritized and escalated for management review	-Assess and approve a risk or issue -Escalate -Execute approved mitigation plan

Objectives

To select a combination of risk response options that will optimize EEOC’s limited resources in managing its portfolio of risks within the bounds of a predefined risk appetite.

Triggers

- Completion of *Evaluate Risks*
- To be performed annually or more often if events warrant (as specified in the triggers for *Establish the Context*)

Inputs

- Analysis of previous and current risk response strategy effectiveness
- Previous communication and training plans
- Prioritized list of risks requiring response options
- Relevant laws and regulations
- Stakeholder analysis

Process participants

- CRO
- ERSC
- ERM Liaisons
- Risk Analysis IPTs
- Risk Owners

Activities

1. Identify risk response options (Risk Owners and Risk Analysis IPTs). Review event trees for those risks listed in the prioritized list of risks requiring response options and identify risk factors that can be mitigated or eliminated to reduce likelihood and severity. Identify consequences that can be mitigated or avoided to reduce likelihood and impact and review existing risk response strategies and controls and insurance policies and analyze their effectiveness. Pinpoint any projects or programs in progress that will impact the existence, likelihood, or magnitude of the risk and observe the project timeline to determine when the risk will be impacted. Document all identified response options for those risk factors and consequences selected.
2. Coordinate risk response option identification (ERM Team). Provide Risk Owners with information about existing risk response options. Assist them in identifying cost effective options including opportunities to extend current risk management activities. Identify opportunities to leverage risk response across Offices to optimize risk management efforts and eliminate any duplicative efforts.
3. Assess risk response options (Risk Owners). Determine the cost of implementing the identified risk response options and evaluate the qualitative impacts that would be reduced or eliminated by the various risk response options using the qualitative impact scales. Compare the residual risk calculation to the risk tolerance level. If the residual risk still exceeds the risk tolerance level, then consider additional risk response options until the estimated residual risk is reduced below the risk tolerance level. Select the most cost effective combination of risk response options that reduces the estimated risk to an acceptable level below EEOC's risk tolerance. Additionally, review the risk response options for compliance with relevant laws and regulations.

Risk response strategies to consider

Avoid Risk	<ul style="list-style-type: none"> a. Discontinue operations or activities in a particular area. b. Prohibit unacceptably high-risk activities and asset exposures through appropriate policies. c. Stop specific activities by redefining objectives, refocusing strategic plans and policies, or redirecting resources. d. Screen alternative projects and budgeted investments to avoid off-strategy and unacceptably high-risk initiatives. e. Eliminate at the source by designing and implementing internal preventive processes.
Accept Risk	<ul style="list-style-type: none"> a. Retain risk at its present level, taking no further action.
Reduce Risk	<ul style="list-style-type: none"> a. Disperse financial, physical, or information assets to reduce risk of unacceptable catastrophic losses. b. Control risk through internal processes or actions that reduce the likelihood of undesirable events occurring to an acceptable level (as defined by management's risk tolerance). c. Respond to well-defined contingencies by documenting an effective plan and empowering appropriate personnel to make decisions; periodically test and, if necessary, execute the plan. d. Diminish the magnitude of the activity that drives the risk. e. Isolate differentiating characteristics to reduce risk. f. Test strategies and implemented measures on a limited basis to evaluate results under conditions that will not influence perceptions of the public. g. Improve capabilities to manage a desired exposure/outcome. h. Relocate operations in order to transfer risk from one location, in which it cannot be well managed, to another location in which it can. i. Redesign the EEOC's approach to managing the risk (i.e., its unique combination of assets and technologies for creating opportunities to achieve mission success). j. Diversify organizational assets that EEOC currently implements for mission and business operations.
Transfer Risk	<ul style="list-style-type: none"> a. Outsource non-core processes (a viable risk transfer option only when risk is contractually transferred). b. Delegate risk by entering into arrangements with independent, capable authorities.

4. Review risk response options with stakeholders (ERM Team and ERM Liaisons). Develop an overall risk response strategy. Consult broadly about risk response with stakeholders. Many response options need to be acceptable to stakeholders or those involved in implementation if they are to be effective and sustainable. Present the risk response options, their costs and benefits, and the recommended risk response strategy to the ERSC for their review and approval.

5. Approve risk response options (CRO and ERSC). Review proposed risk response strategy and selected risk response options and cost-benefit analysis submitted by the ERM Team. Provide comments and feedback to the ERM Team. Obtain permission from the Senior Leadership Team (SLT), Chair, or Chief Operating Officer to seek funding and resources to implement the risk response plans as necessary. In some instances, EEOC may need to obtain permission of OMB, or Congress in order to secure or re-align funding.
6. Prepare risk response option plans (Risk Owners). Develop a detailed risk response action plan including the person responsible for implementing the risk response options, the primary activities, required resources, schedule, budget, reviewer, and status.
7. Implement risk response plans (Risk Owners). **The Risk Owners** will be responsible for working with the Chief Financial Officer (CFO) to secure the budget to implement the risk response plan. Once budget is secured, Risk Owners begin implementation of the risk response and report progress to the reviewer and other identified stakeholders.
8. Monitor risk response option plan implementation (ERM Team). Update information regarding the risk factors and impacts of the risks including annual frequencies, probabilities, impacts, and existing response strategies and controls in the Risk Register. Monitor the status of risk response plans against agreed milestones as recorded. Alert responsible party if deadlines are likely to be or have been missed. Determine and implement corrective action such as *reassigning* work, identifying additional resources to assist with the activity, or communicating with the appropriate individuals to reassign work. See Appendix 3: *Risk monitoring and reporting templates* for examples of reports that can be used to report on the status of risk response plan implementation (this appendix contains a few foundational templates that will be revised and added to as the program is more fully implemented).
9. Enforce implementation deadlines (ERSC). Take corrective action to resolve issues, remove implementation barriers, or address missed deadlines. Set the expectation that deadlines will be met and expected residual risk levels will be achieved.
10. Assess risk response effectiveness (CRO, ERM Team, and ERM Liaisons). Assess whether the reduced probabilities or impacts or other expected benefits have been realized. Make adjustments to the event tree as necessary to reflect actual conditions. Compare the expected benefits and costs of risk response to the actual benefits and costs. Calculate the residual risk and compare it to the risk tolerance levels to determine if additional risk responses will be necessary. Determine the timeline for any additional risk response plans.

Outputs

- Risk response strategies and plans which include the analyzed costs and timelines for development and implementation
- Updated Risk Register with quantified residual risks

Step 6 - Monitor and Review

Overview

The *Monitor and Review* process involves ongoing review of risks to ensure that risk management efforts and response strategies remain relevant and effective. Factors that may affect the likelihood and consequences of an outcome may change over time, as may the factors that affect the suitability or cost of the selected response options. It is therefore necessary to repeat the risk management cycle regularly. Actual progress against risk response option plans provides an important performance measure and should be incorporated into the EEOC's performance management and reporting processes. *Monitor and Review* also involves benchmarking actual ERM risk management outcomes against expected or required performance levels.

Objectives

To continuously monitor the progress of risk response strategies and anticipate and respond to risk events as they occur. Improve EEOC's risk management capabilities, ensure the performance of risk management activities, monitor the progress of risk response strategies, and anticipate and respond to risk events as they occur.

Triggers

- Predetermined timelines for activities as maintained in the risk management calendar
- Occurrence of major risk events or risk factor triggers

Inputs

- KPIs, KRIs, and risk tolerance thresholds
- Risk response strategies and plans which include the analyzed costs and timelines for development and implementation
- Stakeholder input
- Updated ERM Policy, risk appetite statements, roles and responsibilities, organizational structure charts, and ERSC Charter
- Updated Risk Register with quantified residual risks

Process participants

- ERSC
- CRO
- ERM Team
- ERM Liaisons
- Risk Owners

Activities

1. Develop risk monitoring plans (Risk Owners and ERM Team). Develop a risk monitoring plan listing each KRI and KPI. Identify individuals responsible for monitoring the indicators, the associated threshold values, the timing for the monitoring, the required actions should the KRI or KPI breach the threshold, and required alerts and notifications in the event of a breach. Design risk monitoring and reporting templates for internal use and to be provided to a pre-determined

audience. The ERM Team will assist in identifying KRIs and KPIs mapped to multiple risks and resolving any issues around the span of control and monitoring responsibilities. See Appendix 3: *Risk monitoring and reporting templates* for examples of some foundational reports that will be expanded on as the program evolves.

2. Monitor KRIs and respond to changes in risks (Risk Owners). Monitor whether the defined thresholds are breached, or if there has been a change in the indicator signaling a trend, whereby the thresholds might be breached or a risk event might occur. Communicate any breaches or trends requiring corrective action, and take or direct corrective action as appropriate.
3. Coordinate communications and responses to changes in risks (ERM Team). In the event of a KRI or KPI threshold breach or change, determine if the probability of a risk event occurrence has changed that warrants further analysis. Depending on the circumstances, it may be necessary to trigger another process such as *Establish the Context*. Assist the Risk Owners by identifying the broader impacts of a KRI or KPI threshold breach.
4. Record and analyze risk events (Risk Owners, ERM Team, and ERM Liaisons). Record any risk events or near misses to the risk event occurring. Include a description of the event, person responsible for tracking and analysis, the risk category and root cause. Analyze data to identify trends events that could indicate a need for a broader analysis and corrective action beyond the individual risk event in question. The ERM Team will assist in documenting and analyzing risk events and near misses, as well as determining what, if any, corrective action needs to be taken.
5. Review risk event analysis and enforce corrective action (ERSC). For significant risk events related to EEOC's risks, review the risk event analysis paying particular attention to the root cause and timing. Review proposed corrective action and provide input and guidance. The ERSC will perform these steps and inform the Administrator should major risk events occur.
6. Prepare scheduled and ad hoc reports (Risk Owners and ERM Team). Prepare weekly, monthly, quarterly, and annual risk reports. Distribute reports to agreed audience groups according to the agreed schedule. Prepare ad hoc reports for EEOC leadership or Risk Owners upon request.
7. Review and respond to reports (ERSC). Review scheduled and ad hoc risk reports. Note any items requiring corrective action such as risk tolerance or limit breaches, or risk events or near misses. Note changes in the overall enterprise risk profile, in underlying risk types, their root causes, and any trends in changes to risks. Determine if corrective action needs to be taken, the affected parties, and what communications outside of regular channels might be required. Endorse corrective actions and assist in identifying and deploying cross Office/Field Division resources to investigate risk events or sudden changes or developing trends.

Outputs

- Analysis of ERM program effectiveness
- Analysis of the effectiveness of risk response strategies and plans
- Analysis, documentation, and escalation of major risk events
- Changes and enhancements to risk management processes and systems
- ERM Program calendar
- Identified communication and training needs
- Information on major changes in external or internal environment affecting strategic objectives or risk profile
- KRI breaches and risk events
- Scheduled and ad hoc risk reports

Step 7 – Communicate and Learn (Continuous Risk Identification and Assessment)

Overview

Continuous Risk Identification and Assessment are intrinsic to the risk management process and should be considered at each step. An important aspect of the *Establish the Context* process is to identify stakeholders and seek and consider their needs. A communications plan can then be developed to specify the purpose or goal for particular communication needs, identify who is to be consulted and by whom, when communication will take place, how the process will occur, and how it will be evaluated to ensure a continuous flow of information within the Agency. Within EEOC, clear communication channels will be essential in fully integrating all Offices in risk management and in developing a culture where the positive and negative dimensions of risk are recognized and valued.

Objectives

- To improve understanding of risks and the risk management process, ensure that the varied views of stakeholders are considered and build awareness among participants of their active risk management roles and responsibilities.

Triggers

- Annual stakeholder review to be performed each July
- Major change in organizational structure such as a new Program or Office formed
- New requirements, laws, and regulations which EEOC must adhere to or seek to enforce
- Occurrence of a major risk event

Inputs

- Calculated enterprise-wide risk measures for the EEOC's complete portfolio of risks
- Changes and enhancements to risk management processes and systems
- ERM staff and other personnel training needs
- Prioritized list of quantified risks, residual risks, and their interdependencies
- Risk response strategies and plans
- Update Risk Owners
- Updated ERM Policy, risk appetite statements, roles and responsibilities, organizational structure charts, and ERSC Charter
- Updated Risk Register

Process participants

- ERM Team
- ERM Liaisons
- Risk Owners

Activities

1. Manage risk management workflow and schedule (ERM Team). Maintain a calendar of risk management activities for the year beginning with the *Establish the Context* process. Agree on an ERM calendar to communicate schedules, milestones, and expectations of the program. The

calendar will need to be updated at defined intervals as the scope of work is elaborated with EEOC's developing ERM capabilities.

2. Enhance ERM capabilities (ERM Team). Monitor emerging risk management best practices by subscribing to publications, joining consortia and dedicated industry groups, attending conferences, and consulting with other risk professionals at other organizations. Evaluate the effectiveness of existing risk management processes, tools, and techniques. Develop recommendations for enhancements to EEOC's risk management capabilities. Involve the Risk Owners within EEOC and present the recommendations for approval from the SLT, Chair, or Chief Operating Officer, as necessary.
3. Approve ERM capability enhancements (ERSC). Review the proposed risk management capability improvements understanding the benefits and costs. Resolve issues related to performance of the risk management processes raised by the ERM Team.
4. Identify stakeholders, communication, and training needs (ERM Team and ERM Liaisons). Review stakeholder analysis from the previous year and determine if the stakeholder groups have changed. Include both internal and external stakeholders to determine the communication and training needs for each stakeholder group.
5. Provide input on stakeholders, communication, and training needs (Risk Owners). Assist the ERM Team in identifying relevant stakeholders and their communication and training needs. Assist in the development of communication and training content as required. Communicate training needs to the ERM Team and participate in training programs if requested.
6. Develop and deliver communication and training (ERM Team). Develop a detailed communication and detailed training plan including the target audience, the sender, the timing, the communication channel (e-mail, newsletter, meeting, webcast, etc.), the message, and responsibilities for developing and managing the delivery of the content. Develop and deliver the communication and training materials according to plans.
7. Deliver reinforcing messages (ERSC). Review, provide input on, and deliver messages prepared by the ERM Teams. Request endorsing messages from the Chair, as necessary. The purpose is to demonstrate leadership sponsorship for ERM and to promote ERM objectives and benefits to achieving mission success.
8. Maintain ERM inSite presence and process documentation (ERM Team). Maintain the EEOC ERM website. Designate an individual within the ERM Team as the website coordinator. The website coordinator will gather the required content and provide periodic updates to the website.

Outputs

- Changes and enhancements to risk management processes and systems and ERM organizational structure
- Communication and training plans
- ERM website development via the EEOC Intranet
- Stakeholder analyses and stakeholder inputs
- Trainings and communications delivered to the appropriate stakeholders

Appendix 2: Risk Assessment Scales (*Pending review by ERSC*)

Figure 5: Impact/consequence Scale

Descriptor	Description
Very High	Event could be expected to have catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	Event could be expected to have a severe adverse effect on organization operations, organizational assets, individuals, other organizations, or the public. A severe or catastrophic adverse effect means that the event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions for a significant period of time; (ii) severely undermine the ability to perform one or more of the primary functions for a significant period of time; (iii) result in major damage to organizational or critical infrastructure; (iv) result in major financial loss; or (v) result in severe harm to individuals.
Moderate	Event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Public. A serious adverse effect means that the event might: (i) cause a significant degradation in or loss of mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of those functions is significantly reduced; (ii) result in significant damage to organizational or critical infrastructure; (iii) result in major financial loss; or (iv) result in significant harm to individuals.
Low	Event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the public. Limited adverse effect means that the event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of those functions is noticeably reduced; (ii) result in minor damage to organizational, critical infrastructure, or national security assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	Event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals, other organizations, or the public.

Source: Adapted from U.S. Department of Homeland Security (DHS) *National Security Systems Policy Standard Number: 4300B.103-2*, 2013, p. 49.

Figure 6: Initial Probability/Likelihood Scale

Qualitative Values	Best Estimate
Certain	.99
Almost Certain	.93
Probable	.75
Chances About Even	.5
Probably Not	.25
Almost Certainly Not	.07
Impossible	.01

Source: U.S. Department of Homeland Security (DHS) *Transportation Sector Security Risk Assessment (TSSRA)*, 2013, p. 49.

Figure 7: Initial Vulnerability Scale

Qualitative Values	Description
Very High	<ul style="list-style-type: none"> Control effectiveness is very low (e.g., vulnerability estimate of .93) Controls, policies, and procedures are ineffective or insufficient Resources and tools are unavailable or do not meet mission needs No contingency, management, or scenario plans in place One or more major weaknesses exist that render an asset, database, or IT system extremely susceptible to failure or loss
High	<ul style="list-style-type: none"> Control effectiveness is low (e.g., vulnerability estimate of .75) Controls, policies, and procedures are mostly ineffective or insufficient Resources and tools are inconsistently available for mission needs Some contingency, management, or scenario plans in place One or more major weaknesses exist that render an asset, database, or IT system susceptible to failure or loss
Moderate	<ul style="list-style-type: none"> Control effectiveness is medium (e.g., vulnerability estimate of .5) Controls, policies, and procedures are somewhat ineffective or insufficient Resources and tools are available for mission needs but are not optimized Most contingency, management, or scenario plans are in place with limited rehearsals One or more weaknesses exist that render an asset, database, or IT system somewhat susceptible to failure or loss in select areas that can be contained
Low	<ul style="list-style-type: none"> Control effectiveness is high (e.g., vulnerability estimate of .25) Controls, policies, and procedures are mostly effective or sufficient Resources and tools are available and optimized for mission needs, but to a lesser degree for non-mission needs Contingency, management, or scenario plans are in place with some rehearsals Few, easily remediable weaknesses exist that render an asset, database, or IT system susceptible to failure or loss in select areas of lesser consequence
Very Low	<ul style="list-style-type: none"> Control effectiveness is very high (e.g., vulnerability estimate of .07) Controls, policies, and procedures are effective or sufficient Resources and tools are available and optimized for all mission needs Contingency, management, or scenario plans are in place that are rehearsed regularly Very few, minor weaknesses exist that render an asset, database, or IT system susceptible to failure or loss

Figure 8: Initial Speed of Onset Scale

Qualitative values	Definition
Very High	Very rapid onset, little or no warning, instantaneous
High	Onset occurs in a matter of days to a few weeks
Moderate	Onset occurs in a matter of two to three months
Low	Onset occurs in a matter of three to four months
Very Low	Very slow onset, more than four months year to occur

Source: Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Risk Assessment in Practice*, 2004.

Appendix 3: Initial SAMPLE Risk Monitoring and Reporting Templates²

A. Report 1: SAMPLE Simplified (No Risk Score) Risk Register *

Simplified Version Risk Register DRAFT								
FY 2016								
ID	Date Identified	Risk Owner Name	Risk Area	Risk Category	Risk Name	Risk Description	Causal Factors	Impacts
1		OCFO/FSSD (Mohan)	Business Operations	Medium	Clean Audit Opinion	Not maintaining an unmodified/unqualified audit opinion and eliminating all financial material weaknesses and inconsistencies in the financial processes.	Lack of compliance with existing procedures.	Loss of confidence with stakeholders (public, private, OMB and the Hill)
2		OCFO/FSSD (Mohan) and OCFO/BPAD (Krobot)	Business Operations	Medium	Reporting Accuracy	Inability to improve financial reporting processes and procedures that would enhance transparency and accountability for spending for all programs and offices.	Lack of funding.	Loss of confidence with stakeholders (public, private, OMB and the Hill)

* The information in this sample is not intended to represent actual risks at EEOC. A more detailed version of this proposal is available in an expanded format that calculates risk scores. Due to page size constraints it is not represented here. It will be provided as a separate Excel file upon request.

B. Report 2: SAMPLE ERSC Top 10 Risk Snapshot Report*

(Until an Agency-wide analytic/dashboard tool is available this report will be taken from the expanded Risk Register noted in Report 1 notes.)

Enhanced Risk Register														
(DRAFT - All entries are notional in nature and illustrative only)														
Risk Identification and Initial Assessment										Risk Assessment				
Risk ID	Risk Identification Date	Risk Owner (Responsibility)	Risk Category	Risk Name	Risk Description	Causal Factors	Impacts/Consequence	Anticipated Duration (Days/Weeks, etc.)	Risk Trigger	Probability	Impact	Risk Score	Response Action Type	Response Actions
1		OCFO/FSSD (Mohan)	Business Operations	Clean Audit Opinion	Not maintaining an unmodified/unqualified audit opinion and eliminating all financial material weaknesses and inconsistencies in the financial processes.	Lack of compliance with existing procedures.	Loss of confidence with stakeholders (public, private, OMB and the Hill)			Low	High	Medium		
2		OCFO/FSSD (Mohan) and OCFO/BPAD (Krobot)	Business Operations	Reporting Accuracy	Inability to improve financial reporting processes and procedures that would enhance transparency and accountability for spending for all programs and offices.	Lack of funding.	Loss of confidence with stakeholders (public, private, OMB and the Hill)			Medium	Medium	Medium		

* The information in this sample is not intended to represent actual risks at EEOC.

² Future implementation and use of a management and budget analytic platform will allow for dashboard representation of more granular results by other diverse criteria to be determined as the program evolves; currently all reports are manual and Excel based.

C. Report 3: SAMPLE Risk Profile Report*

Risk Profile								
<i>(To be completed for each risk area)</i>								
<i>(Example shown is notional and illustrative only)</i>								
STRATEGIC OBJECTIVE – Deliver Excellent and Consistent Service Through a Skilled and Diverse Workforce and Effective Systems								
Risk	Inherent Assessment		Current Risk Response	Residual Assessment		Proposed Risk Response	Owner	Proposed Risk Response
	Impact	Likelihood		Impact	Likelihood			
EEOC may fail to achieve audit targets due to lack of compliance by Agency staff with existing procedures and regulations.	High	High	REDUCTION: EEOC will develop a program of increased training and technical assistance	High	Medium	EEOC will monitor compliance through quarterly reporting	Primary – OCFO; Secondary - All Program Offices	Primary – Strategic Review
OPERATIONS OBJECTIVE – All Interactions With the Public are Timely, of High Quality, and Informative								
EEOC OCFO staff receive a qualified/modified audit opinion.	High	Medium	REDUCTION: OCFO has developed procedures to ensure compliance with Financial Management policy is monitored and that proper checks and balances are in place.	High	Medium	OCFO will provide training on all aspects of financial management and reporting.	Primary – OCFO; Secondary - All Program Offices	Primary – Internal Control Assessment
REPORTING OBJECTIVE – Provide Reliable External Financial Reporting								
Risk	Inherent Assessment		Risk Response	Residual Assessment		Proposed Action	Owner	Proposed Action Category
	Impact	Likelihood		Impact	Likelihood			
EEOC identified material weaknesses in internal controls.	High	High	REDUCTION: OCFO has developed corrective actions to provide program partners technical assistance.	High	Medium	OCFO will monitor corrective actions in consultation with OMB to maintain audit opinion.	Primary – Chief Financial Officer	Primary – Internal Control Assessment
COMPLIANCE OBJECTIVE – Comply with the Improper Payments Legislation								
Program X is highly susceptible to significant improper payments.	High	High	REDUCTION: OCFO has developed corrective actions to ensure improper payment rates are monitored and reduced.	High	Medium	OCFO will develop budget proposals to strengthen program integrity.	Primary – Program Office	Primary – Internal Control Assessment and Strategic Review

* The information in this sample is not intended to represent actual risks at EEOC.

Appendix 4: ERM Lexicon

The following terms describe core concepts and terms that provides the basis for the EEOC ERM framework and is used extensively throughout the risk management processes outlined in this manual. Many of these terms and definitions are derived from the OMB risk lexicon and have been adapted to apply to an ERM framework appropriate for EEOC.

Figure 9: Proposed Risk Lexicon

Term	Definition
Accidental Hazard	Source of harm or difficulty created by negligence, error, or unintended failure
Adversary	Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities
Control	Strategy or action that is modifying risk
Enterprise Risk Management	Comprehensive approach to risk management that engages organizational systems and processes together to improve the quality of decision making for managing risks that may hinder an organization's ability to achieve its objectives
Establishing the Context	Defining the external and internal parameters to be taken into account when managing risk and setting the scope and risk criteria for the risk management policy
Event	An incident or situation that occurs in a particular place during a particular interval of time
Event tree	Graphic tool used to illustrate the range and probabilities of possible outcomes that arise from an initiating event
Exposure	Extent to which an organization and/or stakeholder is subject to an event
External Context	External environment in which the organization seeks to achieve its objectives
Fault Tree	Graphic tool used to illustrate the range, probability, and interaction of causal occurrences that lead to a final outcome
Economic Consequences	Effect of an incident, event, or occurrence on the value of property or on the production, trade, distribution, or use of income, wealth, or commodities
Hazard	Natural or man-made source or cause of harm or difficulty, may be intentional or accidental
Impact	The extent to which a risk event would affect the enterprise
Intentional Hazard	Source of harm, duress, or difficulty created by a deliberate action or a planned course of action
Internal Context	Internal environment in which the organization seeks to achieve its objectives

Figure 9: Proposed Risk Lexicon (continued)

Term	Definition
Key Performance Indicator (KPI)	Measures on the progress or the achievement of objectives and activities
Key risk Indicator (KRI)	Measures that provide an early warning system that a risk is occurring or has occurred.
Level of risk	Magnitude of a risk or combination of risks expressed in terms of the combination of consequences and their likelihood
Likelihood	Represents the possibility that a given event will occur
Monitoring	Continual checking, supervising, critically observing, or determining the status in order to identify change from the performance level required or expected
Natural Hazard	Source of harm or difficulty created by a meteorological, environmental, or geological phenomenon or combination of phenomena
Probability	Measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty
Residual Risk	Risk that remains after risk management measures have been implemented
Opportunity	The possibility that an event will occur and positively affect the achievement of objectives
Resilience	Ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption
Risk	Potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences
Risk Acceptance	Explicit or implicit decision not to take an action that would affect all or part of a particular risk
Risk Aggregation	The collection of risk (their categories and impact) to develop a more complete understanding of the overall risk
Risk Analysis	Systematic examination of the components and characteristics of risk
Risk Appetite	Amount and type of risk that an organization is willing to pursue or retain
Risk Assessment	Product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making
Risk Avoidance	Informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk
Risk Criteria	Terms of reference against which the significance of a risk is evaluated
Risk description	Structured statement of risk usually containing five elements: sources, events, causes, consequences, and target (if applicable)
Risk Identification	Process of finding, recognizing, and describing potential risks

Figure 9: Proposed Risk Lexicon (continued)

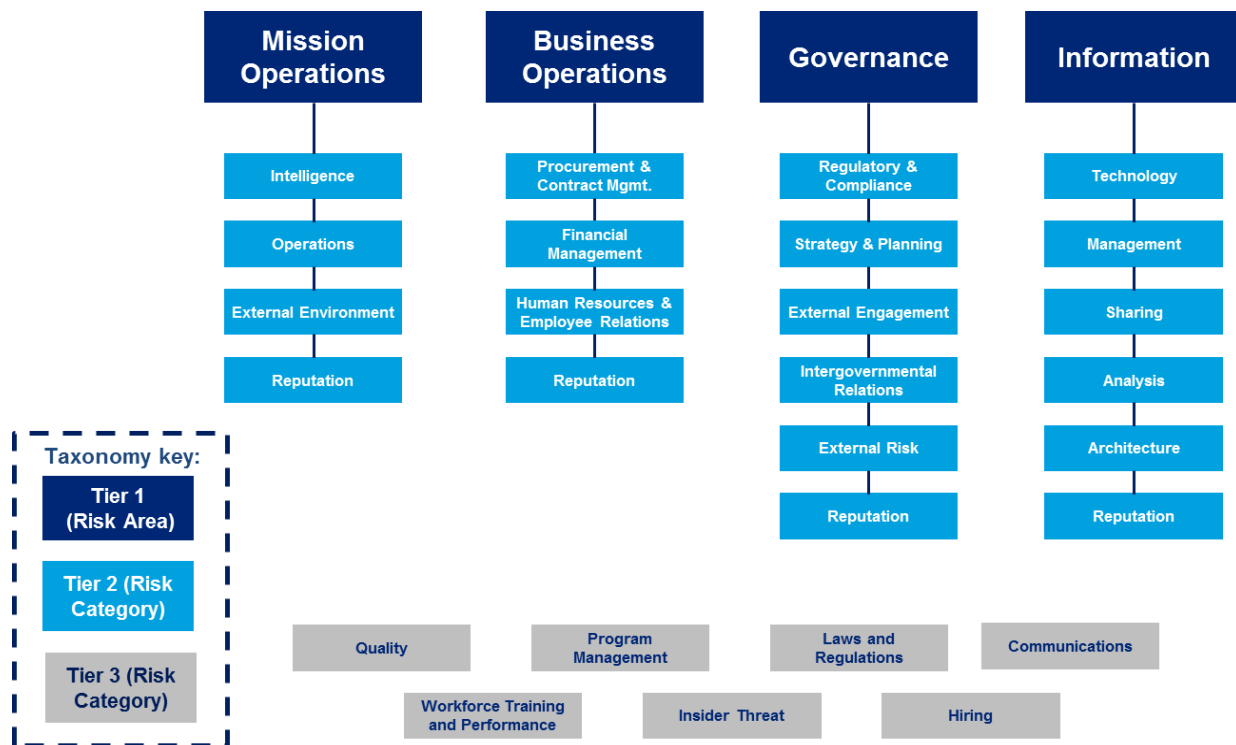
Term	Definition
Risk Management	Coordinated activities to direct and control an organization with regard to risk
Risk Map	Graphic tool used to illustrate areas of risk exposure
Risk Matrix	Tool for ranking and displaying components of risk in an array
Risk Owner	Person or entity with the accountability and authority to manage a risk
Risk Profile	Description of any set of risks
Risk Register	Record of information about identified risks
Risk Reporting	Form of communication intended to inform particular internal or external stakeholders by providing information regarding the current state of risk and its management
Risk Response	Actions defining an organization's approach to an identified risk
Risk Sharing	Form of risk response involving the agreed distribution of risk with other parties
Risk Source	Element which alone or in combination has the intrinsic potential to give rise to risk
Risk Tolerance	Organization's or stakeholder's readiness to bear the risk after risk response in order to achieve its objectives
Risk Transfer	Action taken to manage risk that shifts some or all of the risk to another entity, asset, system, network, or geographic area
Speed of Onset	The time it takes for a risk event to manifest, or the time that elapses between the occurrence of an event and the point at which the enterprise first feels its effects
Stakeholder	Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity
Target	Asset, network, system or geographic area chosen by an adversary to be impacted by an attack
Threat	Natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property
Vulnerability	Susceptibility of the entity to a risk event in terms of environmental factors related to the entity's preparedness, agility, and adaptability

Appendix 5: Proposed ERM Risk Taxonomy

A. General Taxonomy

The ERM Risk taxonomy organizes risk into categories to promote consistent identification, assessment, measurement, and monitoring of risks across the organization. Using common, and consistent, risk taxonomy across the entire organization enables EEOC to determine the relationships between various risks in a manner that allows improved assessment of the overall impact to the organization. Figure 1 illustrates EEOC's general ERM risk taxonomy, including 3 tiers of risk categories. The four tables that follow further define the Tier 2 risk categories within each Tier 1 risk area. Taxonomy tiers are intended to provide increasing levels of detail for a specific risk, and do not denote levels of importance.

Figure 10: Proposed General Risk Taxonomy



B. Taxonomy Risk Area and Risk Category Descriptions

Figure 11: Proposed Risk Taxonomy Category — Mission

Mission Operations	Fundamental areas that are central to, or will influence, EEOC's approach to its core EEO mission
Intelligence	The collection, analysis, production, dissemination, and use of information which allows EEOC to effectively achieve mission success.
Operations	Programs and services (e.g., security screening, regulatory compliance, law enforcement) through which EEOC implements mission objectives.
External environment	Externalities which affect implementation of EEOC mission objectives (e.g., threats, hazards, economic conditions).
Reputation	The common perception that EEOC's stakeholders (e.g., Congress, the traveling public) have about EEOC's mission operations.

Figure 12: Proposed Risk Taxonomy Category — Business operations

Business operations	Core functions or elements that serve to enable how EEOC will carry out its mission through Program Support and Services
Procurement & Contract Management	Procurement, investment and contract management activities performed to support Programs and Services.
Financial Management	Accounting, budget, and financial reporting functions performed to support Programs and Services.
Human Resources & Employee Relations	Workforce recruiting, hiring, training, and deployment to support Programs and Services; Union relations
Reputation	The common perception that EEOC's stakeholders (e.g., Congress, the public) have about EEOC's business operations.

Figure 13: Proposed Risk Taxonomy Category — Governance

Governance	Laws, regulations, and policies which provide the structure and composition for EEOC, including the internal activities and policies for which senior leadership allocates specific aspects of oversight and responsibility
Regulatory & Compliance	Laws, regulations, statutes, Executive Orders, and policies that EEOC is required to comply with in order to carry out operations in support of Programs and Services; this includes reports required by OMB, Congress, and GAO, including internal and external audits, GPRA reporting, and other required metrics and assessments.
Strategy & Planning	The planning or methods EEOC leadership implements for achieving mission goals (usually over the long-term).
External Engagement	The nature of EEOC's third-party relationships (including partnerships) affecting the implementation of EEOC's mission goals.
Intergovernmental Relations	Coordination with other federal (to include Congressional and Administrative branches of government), state, local, tribal, and international governmental bodies and entities on key EEOC initiatives, policies, and programs, as well as rulemaking and legal advisory services to support Programs and Services.
External Risk	Externalities which affect implementation of EEOC operations and governance activities (e.g., political balance, changes in laws and regulations, environmental hazards).
Reputation	Management and promotion of a positive public image and stakeholder beliefs (e.g., Congress, OMB, GAO, and other governing authorities) and opinions of EEOC's mission and mission support activities.

Figure 14: Proposed Risk Taxonomy Category - Information

Information	The technology and functions central to EEOC communications that directly impacts the ability to carry out the mission, business operations, or functions
Technology	The collection of tools – including hardware, software, and modifications to methods and procedures – to address mission and business operational needs.
Management	Technical processes, methods, or policies (including information security) enacted to support Programs and Services with which EEOC accomplishes a mission or business operation objective.
Sharing	Communication, coordination, and information sharing between EEOC components and among stakeholders to promote successful performance of EEOC's mission.
Analysis	Examination and synthesis of information collected and used in mission and business operations.
Architecture	The environment of technology processes and platforms used to collect, manage, share, and organize information to enable mission and business operations.
Reputation	The perception of EEOC's stakeholders regarding EEOC's ability to appropriately secure articulate important information.

Appendix 6: Charter and Implementation Documentation



U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION
Washington, D.C. 20507

Acting Chair
Victoria A. Lipnic

March 24, 2017

MEMORANDUM

TO: General Counsel
Headquarter Office Directors
District Office Directors

FROM: Victoria A. Lipnic *Victoria A. Lipnic*
Acting Chair

SUBJECT: Enterprise Risk Management Policy Statement

In 2016, the Office of Management and Budget updated its Circular A-123 which provides guidance on agency internal financial controls. The circular imposes new requirements on all agencies to formalize and adopt the discipline known as "enterprise risk management" in which a formal framework is created to identify, analyze, prioritize and address risks consistently across their agency as a whole.

The U.S. Equal Employment Opportunity Commission (EEOC) is the leading federal enforcement agency dedicated to stopping and remedying employment discrimination on the basis of race, color, religion, sex, pregnancy, national origin, age, disability, and genetic information or family medical history.

EEOC was created as part of the historic Civil Rights Act of 1964. Title VII of the Civil Rights Act prohibited discrimination on the basis of race, color, religion, sex, and national origin in private sector employment throughout the United States. In over 50 years, our jurisdiction has grown and now includes the following areas: Equal Pay Act of 1963 (included in the Fair Labor Standards Act), Title VII of the Civil Rights Act of 1964, Pregnancy Discrimination Act of 1978, Age Discrimination in Employment Act of 1967, Sections 501 and 505 of the Rehabilitation Act of 1973, Titles I and V of the Americans with Disabilities Act of 1990, Title II of the Genetic Information Nondiscrimination Act of 2008, as well as the Lilly Ledbetter Fair Pay Act of 2009.

I firmly believe that implementing effective risk management principles across all aspects of the EEOC is essential to our successful execution of this mission for the long term.

Our risk management approach must support our ability to identify, analyze, and appropriately respond to strategic risks across the full spectrum of EEOC activities. I have appointed the Deputy Chief Operating Officer as the Chief Risk Officer (CRO) for the EEOC. Additionally, I have directed the Chief Financial Officer, the Chief Information Officer, and the Director of the Office of Research, Information and Planning to develop a framework for the implementation of Enterprise Risk Management (ERM) across the organization. Through ERM, we will:

- Provide a structured, disciplined, and consistent approach to assessing risk.
- Identify strategic risks that threaten EEOC's achievement of our long-term objectives and goals, and manage those risks at the enterprise level through an Enterprise Risk Steering Committee (ERSC) that

is delineated in the ERSC Charter (attached) and the ERM Policy Handbook (under review).

- Ensure that risks are managed in a manner that maximizes the value EEOC provides to the public we serve consistent with defined risk appetite and risk tolerance levels.
- Align our strategy, processes, people, technology, and information to support agile risk management.
- Provide greater transparency into risk by improving our understanding of interactions and relationships between risks in support of improved risk-based decision making.
- Establish clear accountability and ownership of risk.

Risk management must become central to EEOC's mission, vision, and culture. All employees are expected to adopt the principles of risk management developed through the ERM program as it is progressively expanded to all offices and program areas, and to apply the standards, tools and techniques within their assigned responsibilities. With your cooperation and commitment to this policy, EEOC can best ensure the widest application of equal employment practices throughout the nation in the most efficient and cost effective manner.

Attachment: ERSC Charter

cc: Commissioner Chai R. Feldblum
Commissioner Jenny R. Yang
Commissioner Charlotte A. Burrows
Chief Operating Officer, Cynthia G. Pierre
Deputy Chief Operating Officer, Mona Papillon

Equal Employment Opportunity Commission

Executive Risk Steering Committee Charter

March 2017

In 2016, the Office of Management and Budget updated its Circular A-123 which provides guidance on agency internal financial controls. The circular imposes new requirements on all agencies to formalize and adopt the discipline known as "enterprise risk management" in which a formal framework is created to identify, analyze, prioritize and address risks consistently across their agency as a whole.

I. Purpose

The purpose of this charter is to establish the ERSC's overarching responsibility for defining strategy and managing risk at an enterprise level. The ERSC oversees the development and implementation of processes used to analyze, prioritize, and address risks across EEOC. These risks include anything that could impede EEOC's ability to achieve its strategic and mandated objectives. The ERSC is broadly responsible for ensuring that risks are managed to create value for the public we serve and in a manner consistent with established risk appetite and risk tolerances levels. The ERSC has the accountability set forth in this charter, but the responsibility of risk ownership and execution of risk management shall remain in the EEOC offices.

II. Background

Risk management is a key driver for EEOC and affects all aspects of EEOC's operations, policies, and processes. As a federal agency, we are now mandated by OMB to use tools and methodologies to measure risk, and associated risk management activities, throughout the EEOC. This mandate, combined with EEOC's role as the leading federal enforcement agency dedicated to stopping and remedying employment discrimination necessitate the establishment of an executive-level risk governance structure to ensure the most efficient and cost effective use of Federal funds.

III. Function

As EEOC executives, ERSC members are responsible for managing risks within their respective program offices. However, when participating as a member of the ERSC, they are responsible for considering risk management from an Agency-wide perspective. The primary functions of the ERSC are to assist the Chair and the Chief Operating Officer in oversight of key Agency risks through:

- The development, implementation and application of the EEOC Enterprise Risk Management (ERM) Policy;
- Ensuring the effective operation of the EEOC ERM Framework and setting the tone for ERM throughout EEOC;
- Establishing the risk appetite for each major category of risk and the risk tolerance levels for areas of risk associated with EEOC strategic objectives;
- Identifying and reporting of the top strategic enterprise risks; and
- Constant monitoring of EEOC's strategic enterprise risks and the associated response strategies.

The ERSC will fulfill these functions by carrying out the activities detailed in this charter.

IV. Responsibilities and Duties of the ERSC

- In conjunction with the Chief Risk Officer (CRO), defines EEOC's Enterprise Risk Management Framework;
- Defines enterprise risk management priorities based on risk, environment, and opportunities to enhance value for the public we serve through changes to EEOC's approach to operations;
- Sets the risk-based security and risk management strategies for EEOC and provides strategic oversight;
- Provides recommendations to the Chair and Chief Operating Officer regarding the enterprise risk appetite and risk tolerance thresholds;
- Reviews alignment and provides direction for risk strategies based on risk appetite and enterprise risk portfolio;
- Provides recommendations to the Chair and Chief Operating Officer regarding alignment of Agency resources to meet risk strategy objectives and strategic vision;
- Identifies, prioritizes, and monitors the most significant enterprise risks through the strategic risk register and ensures appropriate risk response and mitigation plans are working to achieve desired outcomes;
- Informs the Senior Leadership Team of key risk-based security and risk management decisions;
- Sponsors and provides oversight, direction, and review for the EEOC Risk Assessment working group.

Limitation of Responsibilities and Duties of the ERSC: While the ERSC has the responsibilities and accountability set forth in this Charter, the responsibility of risk ownership shall remain in the program offices.

V. Objectives

The overall goal of the ERSC is to determine an appropriate risk based, crosscutting strategy that will enable the use of EEO framework information to make risk-informed policy and resource allocation decisions across all EEOC functions. The ERSC's primary objective is to develop and oversee an enterprise risk management strategy that achieves the following outcomes:

- **Identify risks** - Compile a unified set of EEO specific risks by risk category. Cast a wide net to understand the universe of risks making up EEOC's risk profile.
- **Develop vulnerability assessment standards and enterprise risk assessment thresholds** – develop a common set of assessment standards across the organization, assessed on likelihood and impact to the organization.
- **Assess risk** - Assign values to each risk using the defined criteria. Initially, the ERSC may use qualitative techniques and then use quantitative analysis for select risks.
- **Assess risk interactions** - Develop a holistic view of risks using techniques such as risk interaction matrices, bow-tie diagrams, and aggregated probability distributions and determine what best suits the Agency's needs.
- **Prioritize risks** - Determine risk management priorities by comparing the level of risk against predetermined target risk levels, risk appetite, and tolerance thresholds.
- **Respond to risks** - Examine response options (accept, mitigate, share, or avoid), perform cost benefit analyses, formulate a response strategy, and develop risk response plans.
- **Create or enhance value** - Use the defined risk appetite and risk thresholds to inform decision making and define the value created by EEOC (e.g., enhanced stakeholder engagements, increased operational efficiency, and enhanced effectiveness) in accomplishing EEOC's missions and achieving strategic objectives.
- **Charter Integrated Project Teams (IPTs) that implement high-priority initiatives:**

- Coordinate and implement internally, as directed, on internal risk management strategies and procedures.
- Coordinate with the various risk-related efforts and those set forth by the EEOC Chair, including working groups and other components as appropriate.

VI. Organization

The ERSC's Chair is the Chief Risk Officer (or designated ERSC Office Director when the CRO is not available) and reports to the Chief Operating Officer. As required, the ERSC oversees the progress of working groups that will consist of executive and staff level participants. Working groups develop detailed plans defining milestones and key deliverables that meet requirements and tasks from the ERSC.

Headquarters Office Directors are permanent ERSC members, and Field representatives will serve two year terms. The Chair will select Field representatives to the ERSC. A term follows the fiscal year cycle.

The ERSC will be composed of the following representatives:

- Chief Risk Officer (CRO) and Committee Chair
- Director, Office of Field Programs
- Director, Office of Federal Operations
- District Director Representative
- Regional Attorney Representative
- Field/ Area/Local Office Director Representative
- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- Director, Office of Research, Information and Planning (ORIP)
- Deputy General Counsel
- Director, Legal Counsel
- Chief Financial Officer (CFO)
- Chief Human Capital Officer (OCHCO)

VII. Responsibilities and Duties

At a minimum, the ERSC shall meet on a quarterly basis. More frequent meetings may be required until ERM is fully engaged across the Agency. Additionally, the ERSC Chair may schedule ad hoc meetings at his or her discretion. ERSC members have the following responsibilities:

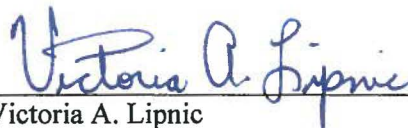
- Attend ERSC meetings in person or virtually if possible. If an ERSC member cannot attend for any reason, he or she must appoint a designated alternate empowered to make decisions on his or her behalf. Should this designee be below Deputy Office Director level, prior approval from the CRO must be obtained.
- Appoint knowledgeable and empowered representatives and a designated alternate to participate in IPTs established by the ERSC.
- Elevate major risk-related decisions to the full ERSC as necessary.
- Review read-ahead materials prior to the meeting.
- Facilitate ERM related communications within their respective program offices.

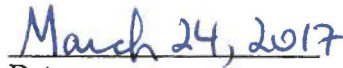
VIII. Decision Making

Decision making will be made through consensus. Should consensus not be able to be reached, the CRO will review the information and contrary opinions and will make the final decision.

IX. Approval.

The EEOC Chair has approved and signed this charter as of the date below.


Victoria A. Lipnic
Acting Chair


Date

EEOC Risk Appetite Statement

EEOC the leading federal enforcement agency dedicated to stopping and remedying employment discrimination on the basis of race, color, religion, sex, pregnancy, national origin, age, disability, and genetic information or family medical history. The EEOC creates value by protecting the rights of the public which we serve. The EEOC ERM policy identifies specific risk management practices that apply to all EEOC Offices at Headquarters, in the field, and to employees at every level of the organization.

EEOC seeks practical and cost-effective solutions to effectively reduce the most significant credible risks that exist that would diminish the value received for every taxpayer dollar spent or degrade our ability to maximize our important role in combating and preventing employment discrimination.

With that in mind, the EEOC has different appetites for different risk types:

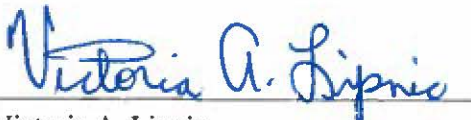
- EEOC is strongly averse to risks that could result in detrimental consequences to the Agency's ability to attain its mission goals.
- EEOC is strongly averse to the compromise of Sensitive Personally Identifiable Information (SPII).
- EEOC is averse to workforce-related risks pertaining to integrity, performance, health and safety, and regulatory compliance.
- EEOC is averse to events that could damage its standing and reputation with the public, U.S. Congress, and other federal and private stakeholders.
- EEOC is risk neutral with regard to other mission and business operational enterprise risks.
- EEOC is risk tolerant to programs that enhance the EEO message across public and private enterprises.


EEOC makes risk informed decisions to achieve its mission within the parameters of its risk appetite:

- EEOC evaluates and manages risks to ascertain and confirm its ability to enforce and educate members of the public and covered employers/entities on topics related to EEO law.
- EEOC considers the interconnected and interdependent nature of the physical, human, and cyber components of enforcing EEO statutes when assessing risks.
- EEOC strikes a balance between countering known risks and hedging against unknown risks by utilizing flexible and realistic mitigation scenarios.
- EEOC evaluates risk levels and implements risk responses and monitoring to bring the risk within tolerance without over controlling related enterprise risks.

Risk appetite is the amount of risk an organization is willing to accept on a broad level in pursuit of its objectives, given consideration of costs and benefits. Risk appetite statements provide guidance on the amount of risk that is acceptable in the pursuit of objectives.

EEOC Risk Appetite Statement: The EEOC operates within a moderate overall risk range. EEOC's lowest risk appetite relates to safety and compliance objectives, including employee health and safety, protection of sensitive personally identifiable information (PII), and compliance with EEO legal requirements.


Victoria A. Lipnic


Date

Enterprise Risk Steering Committee
May 24, 2017, 1:30 – 3:00
6th Floor, Large Conference Room
Minutes

Attendees:

Mona Papillon (Chief Risk Officer and Committee Chair)
Nick Inzeo (OFP)
Carlton Hadden (OFO)
Peggy Mastroianni (Director, Legal Counsel)
Germaine Roseboro (CFO)
Traci DiMartini (OCHCO)
Ron Edwards (ORIP)
Pierette McIntyre (OIT)
Faye Williams (Regional Attorney Representative)
Thomas Coclough (Field/Area/Local Office Director Representative)
Brett Brenner (OCLA)
Sharon Shoemaker (OFP)
Debra Anthony (ORIP)
Ruth Esteban-Muir (ORIP)

Introduction:

Mona Papillon welcomed the ERSC members and provided a summary of the role of the CRO, including the implementation of ERM within EEOC. Mona also noted that the EEOC must recognize, plan for and manage risks across our entire agency; EEOC will set the tone at the top; Integrate ERM with organizational performance management and strategic planning activities; identify and respond to high-priority risks, including aligning resources to address risks; and mature the ERM program over time.

Overview of Enterprise Risk Management:

Debra Anthony provided a brief overview on EEOC ERM Objectives, including increasing the likelihood of success in achieving the objectives of EEOC's mission and strategic plan. Debra described the elements of risk management framework. Debra also noted that EEOC operates within a moderate overall risk range; EEOC is strongly averse to risks that could result in detrimental consequences to the Agency's ability to attain its mission goals; EEOC is strongly averse to the compromise of SPII; and EEOC is averse to workforce-related risk pertaining to integrity, performance, health and safety, and regulatory compliance.

Role of ERSC:

Ron Edwards provided an overview of the ERSC Charter and responsibilities of ERSC members. Ron noted that the ERSC is broadly responsible for ensuring that risks are managed to create value for the public we serve and in a manner consistent with established risk appetite and risk tolerance levels.

Prioritization of risks:

Ruth Esteban-Muir provided an overview of the risk scoring model, and risk profile criteria. Ruth noted that we established questions for determining likelihood and impact to identify crucial risks. Ruth also explained how to complete the risk profile scoring model.

Identification and prioritization of agency risks: (overview of risk profiles)

Office of Field Programs (OFP) – Nick Inzeo presented the following OFP risk profile items:

ACT Digital System incorrect information: If respondent's contact information is incorrect in the ACT Digital System, then EEOC may fail to achieve proper service of charges and other program targets such as ADR offers.

Physical Security of Field Offices: If building and office safety protocols and equipment are not established and maintained, then staff members may be put in danger.

Security of confidential information: If confidential information contained in private sector investigative files is not properly secured, then there is increased risk of data breach and potential significant damage to EEOC's reputation.

Office of Federal Operations (OFO) – Carlton Hadden presented the following OFO risk profile items:

Staff Attrition Impact on Growth of Aged Federal Appeals Inventory: If the Office of Federal Operations (OFO) Appellate Review Program loses too many attorneys by attrition without replacement, then achievement of the strategic/programmatic goal of reducing the aged case inventory will be compromised.

Effective Management of Compliance Inventory: If OFO's Compliance Officers have too large of inventory of compliance cases assigned to them, then relief ordered in appellate decisions will not be implemented and stakeholders will be denied the timely equitable relief that they are entitled to receive.

Investment in Business Intelligence Analytics: If EEOC does not invest in business intelligence services, then it will fail to effectively leverage the wealth of federal sector employment data for general oversight and analysis of EEO issues and trends at the agencies and government-wide.

Office of General Counsel (OGC) – Faye Williams presented the following OGC risk profile submissions:

Contracts approval: If we fail to obtain approval of contracts for expert services in time, then we may not meet court ordered deadlines.

Consent Decree compliance: If the Office of General Counsel does not have a mechanism in place to ensure compliance, then there is a risk that defendants will not honor their obligations under the decrees and future violations could occur.

Office of Legal Counsel (OLC) – Peggy Mastroianni presented the following OLC risk profile submissions:

EEOC FOIA Program statutory processing time limits: If FOIA statutory timelines are not met, then a backlog will occur resulting in delayed issuance of determination, acknowledgment and extension letters and disclosure of responsive documents.

EEOC FOIA Program: If FOIA Xpress crashes or is slow, then this could result in the delay or inability to issue reliable and timely FOIA reports.

Office of Communication and Legislative Affairs (OCLA) – Brett Brenner presented the following OCLA risk profile submission:

Restrictive Language on EEOC appropriation: If Congress approves restrictive language on EEOC appropriations, then that could restrict the agency from carrying out part of our enforcement responsibilities.

The following risk profiles will be reviewed at the next ERSC meeting:

Office of Information Technology (OIT)

Office of Chief Financial Officer (OCFO)

Office of Equal Opportunity (OEO)

Office of Chief Human Capital Officer (OCHCO)

Office of Research Information and Planning (ORIP)

Enterprise Risk Steering Committee
June 5, 2017, 1:00 – 2:30
6th Floor, Large Conference Room
Agenda

Introduction/Recap: Ron Edwards provided a brief recap of the May 24 ERSE meeting.

Identification and prioritization of agency risks: (overview of profiles received) Ron Edwards

Office of Chief Financial Officer (OCFO) – Germaine Roseboro presented the following OCFO risk profile submissions:

Revolving Fund Management Operations: If the revolving fund continues to operate without an OCFO/Chair vetted business plan, then the Agency runs the risk of under/over apportioning funds as well as the very tangible possibility of an Anti-Deficiency Act violation.

Risk Management Process Tool (RMPT): If Interagency Security Committee (ISC) Risk Management Process Tool assessments are not conducted, then staff members may be put in danger.

Office of Chief Human Capital Officer (OCHCO) – Traci DiMartini presented the following OCHCO risk profile submissions:

Centralized Personnel Processing: If all Human Resources (HR) operations are not centralized within the Office of the Chief Human Capital Officer (OCHCO) to ensure the consistent application of HR policies and practices, then we risk our delegated authority.

Electronic Personnel Forms: If personnel files are not properly scanned and uploaded into EOPF, then an adverse impact on EOPF and delays in transferring information to gaining agencies and calculating proper annuity estimates could occur.

Training Data: If EEOC does not have a centralized Learning Management System (LMS), then we may not be in full compliance with OPM standards and reporting requirements.

Human Resources Operations: If the Office of the Chief Human Capital Officer is not sufficiently resourced, then there are significant risks to internal operations and compliance with OPM and OMB requirements.

Office of Equal Opportunity (OEO) – Erica White-Dunston presented the following OEO risk profile submissions:

OEO non-compliance: If the EEO Director does not report directly to the Agency Chair, then Agency fails to comply with MD-110, Chap. 1, Section III, B. If the Agency fails to acknowledge and adhere to the responsibilities of the EEO Director, then the Agency cannot become a model employer and will not be in compliance with 29 CRR 1614.102.

Affirmative employment program staffing and resources: If the Agency fails to provide sufficient staffing and budget to Office of Equal Opportunity (OEO), then OEO will fail to comply with Agency guidance and regulations for EEO offices, and will fail to address its proactive and pre-emptive responsibilities of outreach and training.

Office of Information Technology (OIT) – Pierette McIntyre presented the following OIT risk profile submissions:

Sensitive Personally Identifiable Information (SPII) Datasets: If SPII datasets are not properly secured, then there is increased risk of data breach and potential significant damage to EEOC's reputation.

Unsupported software: If software applications exceed end-of-life maintenance support, then there is increased security and business risk.

Two-Factor Authentication: If two-factor access to Agency systems is not implemented, then there is an increased risk of unauthorized access.

Office of Research Information and Planning (ORIP) – Ron Edwards presented the following ORIP risk profile submissions:

Library resources: If the Library is not adequately resourced, then the Library may not have adequate staffing & resources to assist EEOC staff.

EEO Survey database: If unauthorized access to EEO Survey databases is not prevented, then the confidentiality of stakeholder confidential information is compromised.

Release of Confidential Data: If personnel with access to charge data, survey data and employer's human resource data (including contractors) are not properly trained, then confidential information may be released.

Members were reminded to submit their risk profile scoring sheets NLT COB June 6, 2017.