



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

1.4.60

FEBRUARY 24, 2021

EFFECTIVE DATE

(02-24-2021)

PURPOSE

- (1) This transmits new IRM 1.4.60, Enterprise Risk Management Program.

MATERIAL CHANGES

- (1) IRM 1.4.60.3(1), Enterprise Risk Assessment Process. Edited wording.
- (2) IRM 1.4.60.3(3), Enterprise Risk Assessment Process. Edited wording to clarify that the Risk Working Group (RWG) reviews the risks prior to the Executive Risk Committee (ERC).

EFFECT ON OTHER DOCUMENTS

This IRM 1.4.60 superseded IRM dated August 1, 2019.

AUDIENCE

All Divisions and Functions

Thomas A. Brandt
Chief Risk Officer

1.4.60

Enterprise Risk Management (ERM) Program

Table of Contents

- 1.4.60.1 Program Scope and Objectives
 - 1.4.60.1.1 Background
 - 1.4.60.1.2 Authority
 - 1.4.60.1.3 Responsibilities
 - 1.4.60.1.4 Definition of Terms
 - 1.4.60.1.5 Acronyms
- 1.4.60.2 Enterprise Risk Management (ERM) Program
 - 1.4.60.2.1 Executive Risk Committee (ERC)
 - 1.4.60.2.2 Risk Working Group (RWG)
- 1.4.60.3 Enterprise Risk Assessment Process
- 1.4.60.4 ERM Program Roles and Responsibilities
- 1.4.60.5 Monitoring and Reporting for Enterprise Risks
- 1.4.60.6 ERM Tools and Templates

1.4.60.1
(08-01-2019)
Program Scope and Objectives

- (1) **Purpose:** This IRM section describes the Enterprise Risk Management (ERM) Program and communicates program responsibilities and information resources in support of this program. See IRM 1.4.60.2, Enterprise Risk Management (ERM) Program.
- (2) **Audience:** Servicewide.
- (3) **Policy Owner:** Chief Risk Officer is the policy owner of this program.
- (4) **Program Owner:** Chief Risk Officer is the program office responsible for oversight over this program.
- (5) **Stakeholders:** All business units are stakeholders regarding the ERM Program.

1.4.60.1.1
(08-01-2019)
Background

- (1) Throughout this IRM section, “The ERM Program” refers collectively to the ERM processes, governance bodies (i. e., Risk Working Group [RWG] and Executive Risk Committee [ERC], ERM Liaisons and individuals that support the implementation and operation of ERM at the IRS). “The Office of the CRO (OCRO)” refers to the CRO and the small core team that reports to the CRO.
- (2) The ERM Program, governance and operating structure is based on the industry standard *Committee of Sponsoring Organizations of the Treadway Commission’s (COSO) ERM Framework - Integrating with Strategy and Performance*.

1.4.60.1.2
(08-01-2019)
Authority

- (1) In 2013 the IRS Commissioner established the CRO and responsibility for ERM.
- (2) IRM 1.1.31 outlines the organization and responsibilities of the CRO and the ERM Program.
- (3) OMB Circular A-123 (revised) dated July 15, 2016, *Management Responsibility for Enterprise Risk Management and Internal Control* expanded the focus of the Circular to move Agencies toward an ERM Framework to establish an open, transparent culture that encourages people to communicate information about potential risks and other concerns with their managers without fear of retaliation or blame. The circular requires that each Agency:
 - a. Develop a maturity model approach to the adoption of an ERM framework and a governance structure to effectively implement, direct and oversee operationalizing a robust ERM Program.
 - b. Maintain an enterprise risk profile to provide thoughtful analysis of the risk the Agency faces toward achieving its strategic objectives and arising from its activities and operations. The risk profile assists in facilitating and determining the aggregate level and types of risk that the Agency and its management are willing to assume to achieve its strategic objectives. After initial implementation, the Agency risk profile should be discussed each year with OMB as a component of the summary findings from the Agency strategic review.
 - c. Establish, communicate and periodically review Agency risk appetite. By revisiting and reinforcing risk appetite, the Agency will be positioned to create a culture where organizational goals are consistent with those of leadership, managers and employees.

- d. Review ERM processes and approaches annually for opportunities to refine and improve, ensuring risks are subjected to review with appropriate frequency and that mechanisms are in place to alert appropriate level of management to new or emerging risks as well as changes in already identified risks so that changes can be appropriately addressed.
- (4) OMB Circular A-11 (2015), Section 270, *Performance and Strategic Reviews*, provides ERM guidance for agencies to assess and manage risk as a part of strategic and data driven reviews in support of the broader organizational risk management framework.

1.4.60.1.3
(08-01-2019)
Responsibilities

- (1) See IRM 1.4.60.4, ERM Program Roles and Responsibilities.

1.4.60.1.4
(08-01-2019)
Definition of Terms

- (1) **Risk:** an event that may occur and could negatively affect the achievement of a business objective. Risks are neither good nor bad, and are a normal part of doing business.
- (2) **Enterprise Risk:** an event that may occur and have a significant negative affect on the IRS' ability to achieve its mission, vision and overall objectives.
- (3) **Risk Management:** ongoing process of continuous identification, assessment and prioritization of risk, including decisions about which risks to accept, avoid, transfer or mitigate and followed by monitoring and controlling activities.
- (4) **Enterprise Risk Management:** ongoing process throughout the IRS designed to identify and develop proactive responses (e.g., mitigate, transfer/share, accept, avoid) to enterprise risks before they manifest into larger issues. ERM is influenced by people at every level of the IRS. The results of the risk management process will be used to help define strategy at every level and unit and includes looking at risks from all of Business Units together to identify relationships, connections and themes. ERM also helps the Senior Executive Team (SET) understand how the IRS as a whole is progressing towards meeting its objectives.
- (5) **Enterprise Risk Register:** a template used by the business units when submitting aggregated information from their business unit risk register to the OCRO as part of the annual enterprise risks assessment.
- (6) **Risk Assessment:** process for identifying and assessing risks so that the organization can achieve its objectives. The output of a risk assessment should be an understanding of where the organization may be unprotected against potential negative events. There will always be risks associated with the IRS objectives. However, a risk assessment provides IRS management with the opportunity to evaluate those risks to determine the appropriate risk response.
- (7) **Risk Register:** an expanded template that may be used for a process level or program level risk assessment and contains additional fields that are useful at those levels.
- (8) **Enterprise Risk Assessment:** annual process to collect business unit risk registers, aggregate the results from an enterprise perspective and develop recommendations regarding the enterprise risk profile.

1.4.60.1.5
(08-01-2019)
Acronyms

- (1) This IRM contains the following acronyms and their meanings:

Acronym	Meaning
BPR	Business Performance Review
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CRO	Chief Risk Officer
ERC	Executive Risk Committee
ERM	Enterprise Risk Management
GAO	Government Accountability Office
IRS	Internal Revenue Service
OCRO	Office of the Chief Risk Officer
OMB	Office of Management and Budget
RAFT	Risk Acceptance Form and Tool
RIT	Risk Input Template
RM	Risk Management
RWG	Risk Working Group
SET	Senior Executive Team
TIGTA	Treasury Inspector General for Tax Administration

1.4.60.2
(08-01-2019)
Enterprise Risk Management (ERM) Program

- (1) The ERM Program is authorized by the Internal Revenue Service (IRS) Commissioner and effectuated by management and other personnel, applied in strategy setting and across the enterprise. It is designed to identify potential events that may affect the IRS, to manage risk to be within its risk appetite and to provide reasonable assurance regarding the achievement of the IRS objectives. The Chief Risk Officer (CRO) oversees the ERM Program, which provides an IRS-wide approach to risk management to foster a risk-aware culture and help IRS units incorporate risk management principles into strategies and focus on risk as being one of the core elements of the decision-making framework.
- (2) The ERM governance structure includes an *Executive Risk Committee* comprised of the Deputy Commissioners, the CRO and a small team of senior executives to help the organization identify, monitor and prioritize risks; and a Risk Working Group (RWG) comprised of designated representatives across all IRS organizations (business units) that are responsible for facilitating the process of identifying, aggregating, escalating and recommending responses to risks with support of the OCRO through risk management guidance, training, tools and templates. See IRM 1.4.60.2.1, Executive Risk Committee (ERC) and IRM 1.4.60.2.2, Risk Working Group (RWG).

- (3) The *ERM Program operation* is integrated with the governance model and is designed to enable the day-to-day operations of the program. The ERM program operations is made up of a *small core team* that reports to the CRO and is supported by ERM Liaisons that are considered an extended part of the team but have their direct reporting lines in the business units.
- (4) The *ERM Liaisons* are designated officials that serve as ambassadors/ champions for risk management and support their business unit leadership in identifying, assessing and managing risk that, if not mitigated, will undermine the attainment of their business unit's and/or the IRS's goals and mission. The ERM Liaison reports to their business unit leadership, applying ERM Program direction, and coordinates the activities within their business unit to accomplish the risk management elements set forth by the ERM Program.

1.4.60.2.1
(08-01-2019)
**Executive Risk
Committee (ERC)**

- (1) The ERC is empowered to oversee and guide the efforts of the ERM Program and advise the IRS Commissioner. The ERC provides executive level accountability for identifying, managing and monitoring enterprise risk for the IRS to foster an environment for collaborative and timely risk decision-making, provide transparency to enterprise risks and enable a risk aware culture.
- (2) The ERC meets quarterly to discuss risk and status of the ERM Program. The more specific responsibilities of the ERC include:
 - a. Developing and refining the enterprise-wide appetite/tolerance for risk.
 - b. Providing leadership with respect to communication and training on risk management.
 - c. Reviewing the results of enterprise risk assessments, identifying any additional risks and discussing management priorities for addressing them.
 - d. Understanding the relationships between the different enterprise-wide risks and how they impact one another.
 - e. Monitoring changes anticipated within the external environment, including consideration for new requirements, emerging trends and other factors relevant to the IRS risk profile.
 - f. Understanding the current mitigation strategies in place for enterprise-wide risks and, where appropriate, sponsor assessments/projects to improve and standardize mitigation activities across the IRS.
 - g. Reviewing risk responses for enterprise-wide risks to ensure risks are within the appetite/tolerance of the IRS and identifying whether or not additional actions are necessary.
 - h. Assigning accountability where applicable.
 - i. Monitoring major risk concentrations, key risk indicators and aggregations of enterprise risks through the enterprise risk register, including compliance with stated risk appetite and any material changes in the IRS risk profile.
 - j. Monitoring the periodic identification, assessment and mitigation of risks by the business units.
 - k. Communicating with the ERM Program (including the RWG and ERM Liaisons) to help facilitate the implementation of the ERM Program and evolve risk awareness and mitigation techniques.
 - l. Establishing the RWG to assist the ERC in performing its responsibilities.
 - m. Being the cornerstone for shared knowledge throughout the IRS of enterprise-wide risks.
- (3) Refer to the *ERC Charter* for more detail.

1.4.60.2.2
(08-01-2019)
**Risk Working Group
(RWG)**

- (1) The RWG is established by the ERC to support it in its mission and responsibilities outlined above. The RWG also serves as an interface between the ERC and the business units. The objectives of the RWG are to:
 - a. Serve as enterprise risk leaders, support ERM and the ERC and promote risk awareness at the IRS.
 - b. Foster an environment for candid, informed enterprise risk-related discussion and escalation in supporting the ERC.
 - c. Provide accountability, transparency and oversight for enterprise-level or significant risks and enterprise-wide risk responses as identified by the ERC.
 - d. Reduce operational surprises and enable the IRS to identify emerging risks.
 - e. Provide enterprise risk-related recommendations to the ERC and input/guidance to support risk management efforts as directed by the ERC.
- (2) Refer to the *RWG Charter* for the roles and responsibilities of the RWG.

1.4.60.3
(02-24-2021)
**Enterprise Risk
Assessment Process**

- (1) Enterprise risk assessment is a dynamic and iterative process for identifying and assessing risks to the achievement of the IRS objectives. There will always be risks associated with the IRS objectives. The enterprise risk assessment provides IRS management the opportunity to evaluate those risks to determine the appropriate risk response based on risk appetite.
- (2) The CRO in conjunction with the ERC and RWG periodically reevaluates the approach to and methodology used for the enterprise risk assessment to identify necessary changes or areas for improvement.
- (3) Annually, the OCRO facilitates an enterprise risk assessment at the IRS. The high-level process is outlined below:
 - Each business unit submits an up-to-date business unit-level risk register using the enterprise risk register template. The business unit risk submissions are aggregated and evaluated to form the foundation for the enterprise risk assessment.
 - Proposed enterprise risks are scored for likelihood and impact using a combination of qualitative and quantitative methods including current risk response. Likelihood represents the possibility that a given event will occur, while impact is the result or effect of an event.
 - After RWG review, the ERC evaluates the proposed Enterprise Risk Profile adjusting risk descriptions, scores, etc. based on their collective expertise and finalizes the risk profile.
- (4) The annual enterprise risk assessment approach is designed to provide timely information about enterprise and business unit risks as input to strategic, investment and performance planning processes.
- (5) The enterprise risk assessment process and timeline are reviewed and adjusted annually based on feedback of Business Unit Leadership and ERM Liaisons. The process is comprised of several steps and generally includes:
 - a. gathering risk registers from units
 - b. analysis and aggregation of business unit risk information by the OCRO
 - c. review and analysis of aggregated risk information by the RWG
 - d. scoring likelihood and impact of enterprise risks

- e. deliberation of enterprise risk assessment output by the ERC for determination on priority and focus of mitigation and monitoring for the upcoming year and update of the IRS Enterprise Risk Profile

1.4.60.4
(08-01-2019)

ERM Program Roles and Responsibilities

- (1) **The Chief Risk Officer (CRO)** oversees the ERM Program which provides an IRS-wide approach to risk management to foster a risk-aware culture and helps the IRS incorporate risk management principles into strategies, providing senior management the information necessary to more effectively make sound decisions, focusing on risk as being one of the core elements of the decision-making framework. The CRO is responsible for:

- a. Communicating and continuing to evolve and mature ERM pursuant to the IRS ERM vision.
- b. Participating in IRS strategy and objective setting discussions, including strategic planning and decision-making forums, providing risk perspective.
- c. Establishing ERM framework, structure and process including defining roles and responsibilities.
- d. Ensuring proper risk management ownership by the business units.
- e. Guiding integration of ERM with other IRS planning and management activities.
- f. Promoting risk awareness at the IRS.
- g. Partnering with the business and functional units on their most important risks.
- h. Reporting to the IRS Commissioner on the progress of the ERM Program, status of enterprise risks and recommended actions.
- i. Representing the IRS in the Treasury ERM Council, the Federal Inter-agency ERM Council and other forums.

- (2) **Division Commissioners, Chiefs, Heads of Commissioner Direct Report Organizations** are responsible for:

- a. Setting the tone at the top for risk management, creating a safe environment which encourages transparent risk identification by staff and managers from across the IRS and is supportive of open risk discussions.
- b. Designating an *ERM Liaison* to serve as an ambassador/champion for risk management for the business unit and focal point for the OCRO and ERM Program.
- c. Motivating employees to embrace risk management and providing them with the tools and training to do so.
- d. Understanding and accepting responsibility for identifying, assessing and managing risk.
- e. Encouraging the integration of risk in the decision-making process.
- f. Promoting ERM awareness through transparency in all directions, and sharing of IRS and business unit ERM successes and best practices.
- g. Owning risks and management of the risks associated with the business unit, programs and “upstream/downstream” activities.
- h. Engaging and collaborating in risk identification and assessment processes and activities.
- i. Driving prioritization of mitigation strategies and plans.
- j. Supporting the implementation of mitigation activities to address open risk exposures.
- k. Supporting and empowering the ERM Liaison in the development of risk reporting.

- l. Reporting on business unit and enterprise risks to the ERM Liaison.
- m. Communicating the priority of ERM/RM and supporting the ERM Liaison in establishing a safe environment in their business unit workgroups.
- n. Encouraging communication of risks identified upward as necessary and communicating risks with unit leadership and the ERM Liaison.
- o. Encouraging employees to understand their ability to communicate risks to the ERM Liaisons and management.

(3) **Managers at All Levels** are responsible for:

- a. Contributing to a safe environment which encourages transparent risk identification and is supportive of open risk discussions.
- b. Supporting risk awareness through transparency in all directions and sharing IRS and business unit risk management successes and best practices.
- c. Encouraging others to embrace risk management.
- d. Considering risk as a factor in daily decisions.
- e. Identifying and assessing risks within the business unit and elevating them, as necessary.
- f. Owning certain risks at the unit or process level.
- g. Supporting the prioritization and implementation of mitigation activities.
- h. Executing certain mitigation activities (e.g., approvals, authorizations and review activities).
- i. Facilitating the design and implementation of mitigation responses and activities.
- j. Participating in research, analysis or mitigation planning.
- k. Monitoring the progress and effectiveness of mitigation plans.
- l. Reporting on business unit and enterprise risks to the ERM Liaison or through their defined ERM process.
- m. Communicating the priority of ERM/RM and supporting the ERM Liaison in establishing a safe environment in their business unit workgroups.
- n. Encouraging communication of risks identified upward as necessary and communicating risks with unit leadership and the ERM Liaison or through their defined ERM process.
- o. Supporting unit leadership and the ERM Liaison with tailoring risk communications specific to the business unit.

(4) **ERM Liaisons** are responsible for:

- a. Acting as an ambassador/champion for risk management, encouraging a safe environment which encourages transparent risk identification by staff from across the business units and is supportive of open risk discussions.
- b. Facilitating the integration of risk in the decision-making process.
- c. Facilitating communications between the OCRO and unit leadership and employees.
- d. Supporting ERM awareness through transparency across the agency.
- e. Supporting the evolution and maturation of the ERM Program by ensuring the right structure and processes exist throughout the business unit at every level to identify and share or elevate risks.
- f. Supporting the identification of risk by unit members based on knowledge, skills or experience as appropriate.
- g. Maintaining Risk Registers and Key Risk Indicators for their unit, on behalf of the unit Commissioner, Chief or Director.

- h. Enabling risk identification and assessment activities occur with visibility to the program and process level.
- i. Tracking risk responses for mitigation timeliness, completeness and accuracy and appropriate ownership.
- j. Coordinating unit risk activities (i.e., identification, assessment and mitigation) with other IRS units.
- k. Advising on the design and implementation of mitigating response and activities.
- l. Monitoring unit and enterprise risks and mitigation efforts to ensure successful mitigation of shared risks.
- m. Reporting unit and enterprise risks to the OCRO.
- n. Supporting unit leadership and sharing information with internal stakeholders, the OCRO and other unit ERM Liaisons.
- o. Planning, designing and delivering risk communication between the ERM Program and unit leadership and employees.
- p. Sharing IRS and business unit ERM successes and best practices in their business unit.

(5) **IRS Employee** opportunities to support IRS Risk Management efforts include:

- a. Contributing to a safe environment within the workgroup where risks are identified and discussed openly.
- b. Embracing risk management and encouraging others within the business unit workgroup to do the same.
- c. Considering risk as a factor during regular work activities.
- d. Working to identify risk in performing daily tasks.
- e. Identifying and appropriately referring workgroup issues.
- f. Participating in solving workgroup issues.
- g. Performing daily activities which include performing controls (i.e., reconciliations or checklists) aimed at mitigating or preventing risks.
- h. Possibly providing status updates of risks within the workgroup.
- i. Identifying and communicating risks to management.
- j. Receiving and considering training and other risk communications delivered by their managers, IRS Leadership, the ERM Program or others.

1.4.60.5
(08-01-2019)
Monitoring and Reporting for Enterprise Risks

- (1) Enterprise risk reporting refers to the reporting of enterprise risk information up through each organization to their respective Commissioner, Chief or Director through Business Performance Reviews (BPRs) or other program updates and to executive committees.
- (2) The OCRO collects enterprise risk updates through multiple channels, including but not limited to identified points of contact, ERM Liaisons, BPRs and executive committee reporting.

1.4.60.6
(08-01-2019)
ERM Tools and Templates

- (1) The *OCRO website* provides access to background material, communication and awareness materials such as podcasts and discussion questions, as well as tools and templates that have been developed to facilitate the enterprise risk assessment process as well as assist ERM Liaisons and business units in the consideration of risk in their business unit as well as in conducting risk assessment activities specifically. Some of the tools and templates are highlighted in the following.
- (2) The *Risk Assessment Guide and Toolkit* outlines an approach, tips and tools to enable a repeatable process for risk assessments and can be used to facilitate

risk identification and risk assessments at the program, process and business unit levels. In addition to being used at various levels of the organization, the Risk Assessment Guide and Toolkit can be used at various points within the risk assessment lifecycle.

- (3) The *Enterprise Risk Assessment Template (Risk Register)* provides a consistent framework to document risk information for business units to maintain and provide to the OCRO for enterprise risk assessment updates. Business units, programs and project teams can incorporate additional fields in their register to fit the needs of a particular risk assessment and/or their own internal monitoring and reporting purposes.
- (4) The *Risk Acceptance Form and Tool (RAFT) (Form 14675)* provides a consistent framework that can be leveraged within a unit's existing governance or management approval processes to clearly document business decisions in the context of risk appetite and/or acceptance. Specifically, the RAFT can be used as a framework to assess various options in making decisions for achievement of objectives, a guide to articulate rationale behind those decisions within the context of risk appetite and a documentation trail to support these business decisions.
- (5) The *Risk Input Template (Form 14679)* is used to capture information about a potential risk to facilitate discussion throughout the risk consideration process. The risk consideration process provides a formalized process for organizations to consider and when necessary, elevate risks which may have an enterprise-wide impact and collaborate with appropriate stakeholders to provide transparency into the risks facing the organization and help reduce operational surprises.
- (6) The *Enterprise Risk Channel (Form 15201)* exists to facilitate the identification of risk by all employees of the IRS. This channel allows for the confidential identification of risks directly to the OCRO.

