



Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Audit Report

Social Security Administration's
Enterprise Risk Management

022323 August 2024



Office of the Inspector General

SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: August 5, 2024

Refer to: 022323

To: Martin O'Malley
Commissioner

From: Michelle L. Anderson *Michelle L. Anderson*
Assistant Inspector General for Audit
as Acting Inspector General

Subject: Social Security Administration's Enterprise Risk Management

The attached final report presents the results of the Office of Audit's review. The objective was to determine whether the Social Security Administration's Enterprise Risk Management program complies with Office of Management and Budget *Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*.

Please provide within 60 days a corrective action plan that addresses each recommendation. If you wish to discuss the final report, please call me or have your staff contact Mark Searight, Deputy Assistant Inspector General for Audit.

Attachment

Social Security Administration's Enterprise Risk Management

022323



August 2024

Office of Audit Report Summary

Objective

To determine whether the Social Security Administration's (SSA) Enterprise Risk Management (ERM) program complies with Office of Management and Budget (OMB) *Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*.

Background

As of Fiscal Year (FY) 2017, following the issuance of revised OMB *Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*, Federal agencies have been required to implement an ERM capability in coordination with the strategic planning processes required by the *Government Performance and Results Act Modernization Act* and the internal control processes required by the *Federal Managers' Financial Integrity Act* and the Government Accountability Office's *Standards for Internal Control in the Federal Government*.

ERM is an agency-wide approach to addressing internal and external organizational risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks within silos. To help guide and evaluate its implementation, SSA developed a maturity model with five distinct phases, starting at Initial and ending at Advanced, which indicates a mature ERM.

Results

SSA is complying with *Circular A-123* ERM requirements; however, its ERM capability is less mature than expected based on the implementation plans it created in accordance with OMB guidance. As of FY 2023, 6 years after OMB's ERM guidance became effective, SSA is at the Emerging phase, the second of five maturity levels. SSA initially planned to reach ERM maturity, the fifth or Advanced level in FY 2024 but later revised its maturity date to FY 2028. While OMB guidance does not require that ERM be implemented by a certain date, SSA has delayed its previously planned maturity date and appears to be behind schedule to meet the FY 2028 date.

SSA formed an ERM team, but it did not provide that team sufficient resources. This contributed to the Agency missing and extending deadlines in its *ERM Implementation Plan*. SSA's ERM governance structure, which should have overseen the Agency's ERM program, did not make timely decisions on program governance, which impacted achievement of milestones and ERM maturity. The governance structure also has not promoted incorporating risk awareness (a critical part of ERM) throughout SSA's operations.

Without a mature ERM, SSA continues to manage risks in separate silos, not collaboratively, hindering a risk-aware culture and a common understanding of risk across the Agency. This limits SSA's ability to holistically identify, analyze, evaluate, respond, and manage the risks that could impede its mission and ability to serve its customers.

Recommendations

We recommend SSA make ERM implementation a priority by providing the ERM team the resources it needs to ensure ERM reaches maturity no later than the planned date of FY 2028, in accordance with its current *ERM Implementation Plan* and that it ensure as it is working toward reaching maturity that the Enterprise Risk Management Council is providing leadership over the ERM program and that key *Circular A-123* requirements are completed. SSA agreed with our recommendations.

TABLE OF CONTENTS

Objective.....	1
Background.....	1
Scope and Methodology	3
Results of Review	4
Enterprise Risk Management Implementation	4
Implementation Plan Delays.....	6
Enterprise Risk Management Resources	7
Enterprise Risk Management Governance	7
Risk Appetite and Tolerance Levels	8
Promoting Risk Awareness.....	8
Recommendations	9
Agency Comments.....	9
Appendix A – Scope and Methodology	A-1
Appendix B – Enterprise Risk Management Implementation Structure	B-1
Appendix C – Maturity Evaluation Score Range.....	C-1
Appendix D – Agency Comments.....	D-1

ABBREVIATIONS

DC	Deputy Commissioner
ERM	Enterprise Risk Management
ERMC	Enterprise Risk Management Council
FY	Fiscal Year
GAO	Government Accountability Office
KPI	Key Performance Indicator
KRI	Key Risk Indicator
OIG	Office of the Inspector General
OMB	Office of Management and Budget
Pub. L. No.	Public Law Number
SSA	Social Security Administration

OBJECTIVE

Our objective was to determine whether the Social Security Administration's (SSA) Enterprise Risk Management (ERM) program complies with Office of Management and Budget (OMB) *Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*.¹

BACKGROUND

OMB has emphasized the importance of having appropriate risk management processes and systems that identify challenges early, bring them to the attention of agency leadership, and develop solutions. To that end, in July 2016, OMB revised *Circular A-123* to ensure Federal managers are effectively managing agency risks and are providing policy changes that modernize existing efforts.² *Circular A-123* requires that agencies implement an ERM capability coordinated with (1) strategic planning and a strategic review process established by the *Government Performance and Results Act Modernization Act*³ and (2) internal control processes required by the *Federal Managers' Financial Integrity Act*⁴ and *Standards for Internal Control in the Federal Government*, known as the Green Book.

Circular A-123 defines ERM as an effective agency-wide approach to addressing the full spectrum of the organization's internal and external risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks within silos. ERM should be forward-looking and designed to help managers make better decisions, alleviate threats, and identify unknown opportunities to improve the agency's value to the taxpayer and increases its ability to achieve its strategic objectives.⁵ While an agency may not be able to respond to all risks related to achieving its strategic objectives, it must identify, measure, and assess risks related to its mission delivery, creating an environment that encourages employees to communicate information about potential risks without fear of retaliation or blame.⁶

¹ Throughout the report, we refer to OMB *Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*, as *Circular A-123*.

² The revised *Circular A-123* superseded all prior versions. It was effective for Fiscal Year (FY) 2016 but made ERM implementation requirement effective FY 2017. OMB, *Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, M-16-17*, p. ii (July 15, 2016).

Until SSA has fully implemented an ERM approach to risk management, it may continue providing the existing risk-assurance statements to its Office of the Inspector General (OIG) and/or private accounting firms, as appropriate. OMB, *Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, M-16-17*, part II, section C, p. 21 (July 15, 2016).

³ *GPR Modernization Act of 2010*, Pub. L. No. 111-352, § 124 Stat. 3866-84 (2011).

⁴ *Federal Managers' Financial Integrity Act of 1982*, Pub. L. No. 97-255, § 96 Stat. 814-15 (1982).

⁵ OMB, *Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, M-16-17*, Attachment, p. 1 and part II, p. 10 (July 15, 2016).

⁶ Per *Circular A-123*, "The responsibilities of managing risks are shared throughout the Agency from the highest levels of executive leadership to the service delivery staff executing Federal programs." OMB, *Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, M-16-17*, part II, sec. A, p. 12 (July 15, 2016).

Per *Circular A-123* guidance, SSA should tailor its ERM to meet its specific needs, while addressing the issues of ERM governance, risk profiles, and implementation, as follows:

- SSA's ERM governance structure consists of its senior leaders and is the governing body over SSA's ERM program.⁷ The governing body should ensure risk oversight, including developing the Agency's annual risk profile, risk assessments, risk appetite, and tolerance levels that support SSA's strategic goals and objectives.⁸ SSA's ERM governance structure should set the tone at the top, demonstrating its support and commitment to the Agency's risk management philosophy and how it considers risk in its day-to-day activities and decision making.
- SSA's risk profile should guide decision making based on the Agency's risk appetite and risk tolerance levels. It should include a prioritized inventory of its most significant risks,⁹ be updated annually, identify options to address significant risks, and be approved by the ERM governance structure.
- SSA should develop an ERM maturity model implementation approach.¹⁰ *Circular A-123* encouraged SSA to develop an approach to implement ERM starting in FY 2016, continuously building risk-identification capabilities to identify new or emerging risks and/or changes in existing risks in FY 2017 and each year thereafter.¹¹

In response to *Circular A-123*, SSA developed a maturity model to guide its ERM implementation and maturity progress (see Figure 1).¹² The model has five phases, starting at Initial and ending at Advanced, which indicates a mature ERM.¹³

⁷ *Circular A-123* provides SSA discretion with governing its risk-management function, which may include a Risk Management Council. The Council should be chaired by SSA's Chief Operating Officer or a senior official with responsibility for the enterprise. OMB, *Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, M-16-17*, p. 2 and part II, sec. A, pp. 12-13 (July 15, 2016).

⁸ Adapted from the Committee of Sponsoring Organizations of the Treadway Commission ERM framework, *Circular A-123* defines risk appetite as 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. OMB, *Circular A-123* defines risk tolerance as 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. OMB, *Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, M-16-17*, part II, p.10 (July 15, 2016).

⁹ OMB, *Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, M-16-17*, part II, sec. B, pp. 13 and 14 (July 15, 2016).

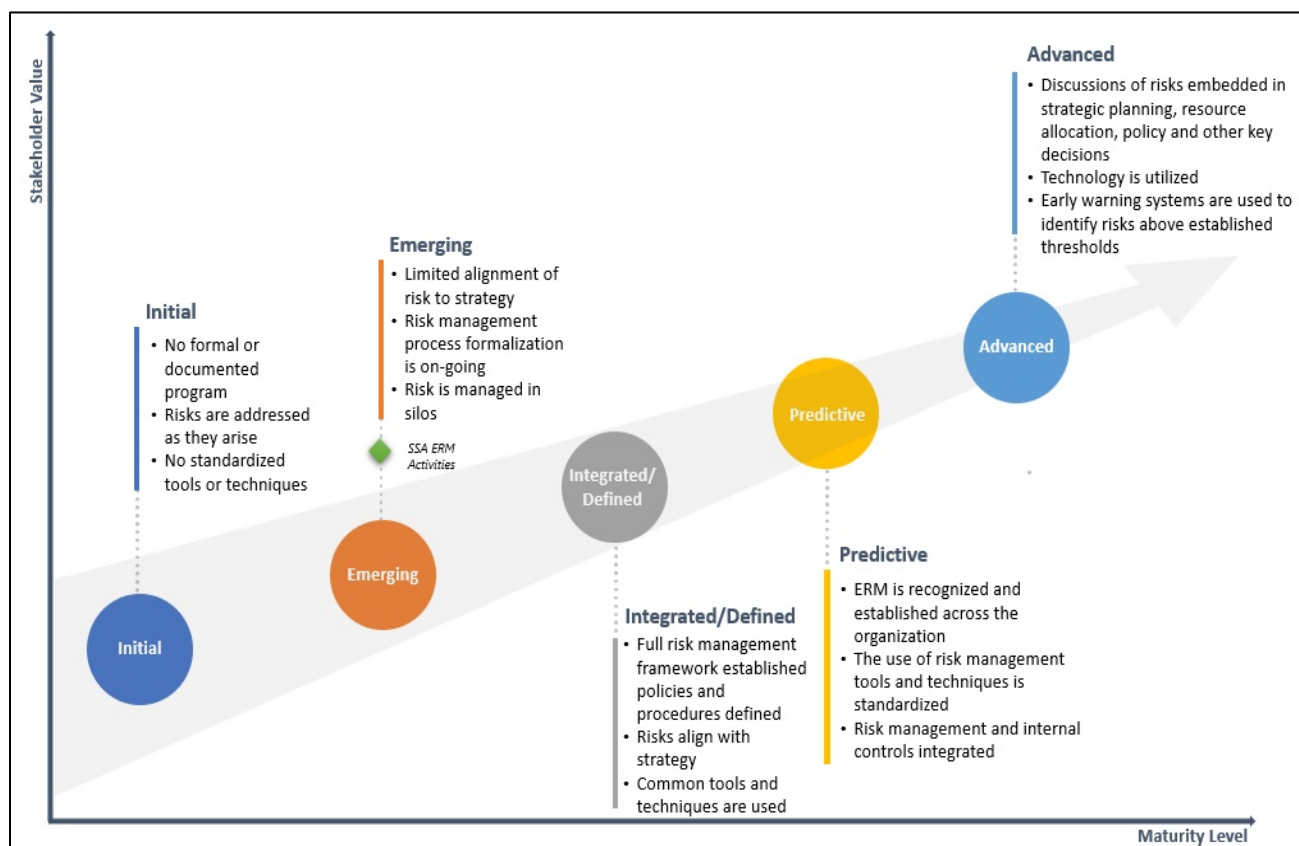
¹⁰ A maturity model allows an agency to assess itself at different levels to determine its progress toward achieving ERM maturity.

¹¹ *Circular A-123* does not require, but does encourage, agencies to develop an approach to implement ERM that may include a planned risk governance structure; process for considering risk appetite and tolerance levels; methodology for developing a risk profile; and general implementation timeline, and plan for maturing the comprehensiveness and quality of the risk profiles over time. OMB, *Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, M-16-17*, part II, section C, p. 20 (July 15, 2016).

¹² As *Circular A-123* guidance referenced, SSA adapted its Maturity Model from the Risk Management Society. The Model includes 80 fundamental activities related to 7 specific task areas that are organized into 4 key implementation phases to support ERM implementation and maturity over a projected 5-FY period. For more information about SSA's ERM implementation structure, see Appendix B.

¹³ For more information about the five levels, see Appendix C.

Figure 1: SSA Maturity Model as of FY 2023¹⁴



SSA developed its initial *ERM Implementation Plan* in December 2019. Per the *Plan*, SSA planned to reach ERM maturity, the fifth or Advanced level in its ERM maturity model, in FY 2024. SSA revised its *ERM Implementation Plan* in FY 2022, pushing the date in which it planned to reach ERM maturity to FY 2028.

SCOPE AND METHODOLOGY

We reviewed SSA’s ERM implementation through FY 2023 to determine its maturity phase and whether it included key elements, such as initial risk identification, risk analysis and evaluation, the development of alternatives to respond to risks, and continuous risk identification.¹⁵ We also met with SSA subject-matter experts who were responsible for or knowledgeable of SSA’s ERM program.

¹⁴ The maturity model is taken from SSA’s *Integrity Act Handbook*.

¹⁵ Based on HM Treasury, *The Orange Book, Management of Risk – Principles and Concepts*, p. 13 (2004). OMB, *Circular A-123, Management’s Responsibility for Enterprise Risk Management and Internal Control, M-16-17*, part II, p. 11 (July 15, 2016).

RESULTS OF REVIEW

SSA is complying with *Circular A-123* ERM requirements; however, its ERM capability is less mature than expected based on the implementation plan it created in accordance with OMB's guidance. At the time of our review, SSA had reached the Emerging phase, the second of five maturity levels. In FY 2020, SSA planned to reach ERM maturity in FY 2024, later revising its maturity date to FY 2028. While OMB's guidance does not require implementation by a certain date, SSA has delayed its maturity date previously and appears to be behind its current schedule to meet the FY 2028 date.¹⁶

Enterprise Risk Management Implementation

SSA has accomplished several activities towards ERM implementation as follows:

- Designated ERM authority and responsibility to its Deputy Commissioner for Budget, Finance, and Management.
- Established an Enterprise Risk Management Council (ERMC) senior executive committee to oversee and promote its ERM program and advise the Commissioner on risk-related issues.¹⁷
- Developed the OMB-recommended ERM framework that included tools, templates, and standard operating procedures for pertinent staff to carry out risk assessment processes.
- Developed an *ERM Implementation Plan* to guide completion of activities needed to implement and mature its ERM framework, targeted for FY 2028.
- Developed a maturity model to evaluate its progress toward the Advanced phase of maturity.
- Developed its initial risk appetite to define the acceptable amount of risk it is willing to take with no or minimal impact to its operations.¹⁸
- Developed an *ERM Training Plan* and *ERM Communications Plan* designed to further ERM maturity by increasing employees' ERM awareness and ensuring staff with ERM responsibilities have the knowledge and skills to carry out ERM activities.

¹⁶ *Circular A-123* encourages agencies to develop an approach to implement ERM, as soon as practicable, before June 2, 2017. SSA's initial *ERM Implementation Plan* was documented in December 2019. The Plan outlined its ERM Framework's implementation over a 5-FY period. Per SSA's *ERM Implementation Plan*, the Plan was developed ". . . to assist in driving ERM Implementation forward by building repeatable processes for risk management, developing a risk-aware culture, and integrating risk management within our goal of continuous improvement." SSA, *Enterprise Risk Management Fiscal Year 2023-2027 Implementation Plan*, p. 2, (July 2022).

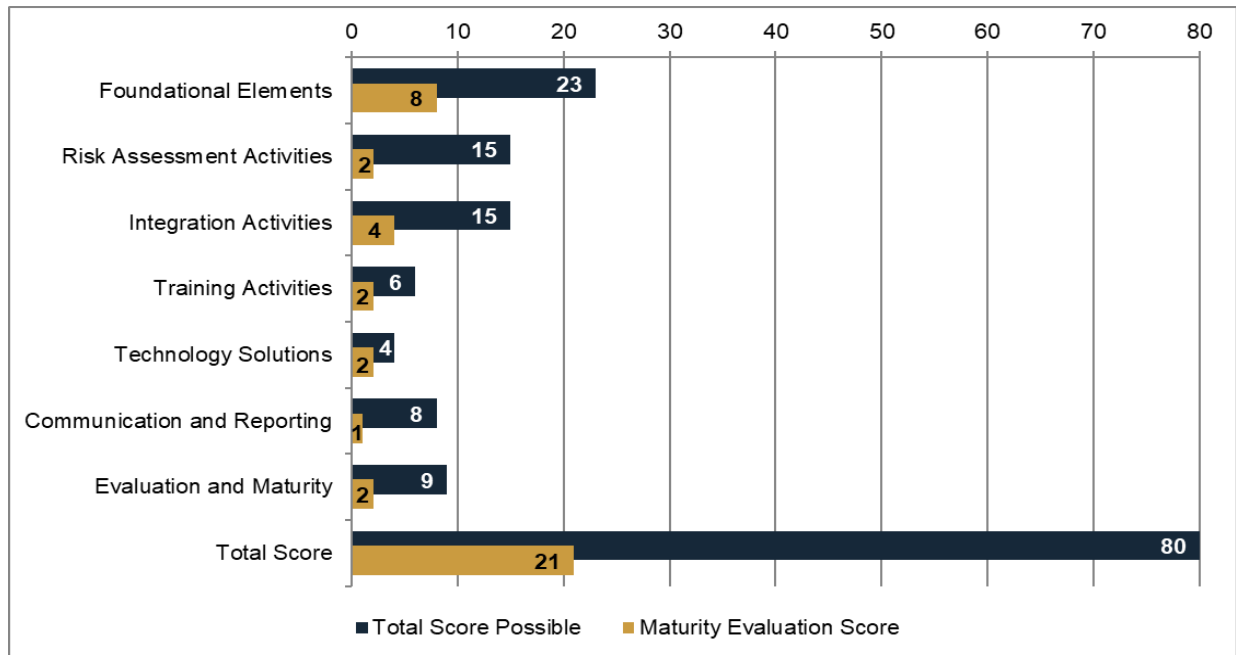
While *Circular A-123* does not provide a specific timeline for agencies to implement ERM, it does provide a process should ERM not be fully implemented. SSA reported it was impacted by several challenges over the last several years, including the pandemic as well as funding issues and staffing losses; therefore, it may not achieve its target FY 2028 maturity date as planned.

¹⁷ SSA established its ERMC in FY 2020. Before FY 2020, SSA used other executive committees and its ERM team to oversee ERM.

¹⁸ SSA finalized the development of its risk appetite in June 2021. As of FY 2023, SSA was revising its risk appetite to reflect changes to its leadership, external environment, and ERM program that have occurred since FY 2021.

SSA completed 21 of 80 activities it included in its maturity model to help evaluate its progress towards ERM maturity (see Figure 2).

Figure 2: Maturity Model Evaluation Score Results by Task Area¹⁹



While SSA made progress in all task areas, its progress in most has been incrementally slow over the last 3 FYs (see Table 1).

Table 1: ERM Progress for FYs 2021 Through 2023

Task Area	FY 2021 Maturity Score	FY 2022 Maturity Score	FY 2023 Maturity Score	Percent of Score Points Obtained as of FY 2023
Foundational Elements	4	5	8	35%
Risk Assessment Activities	4	2	2	13%
Integration Activities	4	3	4	27%
Training Activities	0	2	2	33%
Technology Solutions	0	2	2	50%
Communication and Reporting	0	1	1	13%
Evaluation and Maturity	2	2	2	22%
Total Score	14	17	21	26%

¹⁹ Score results are as of September 30, 2023. For more information on these activities, see Table 1 and Appendix B, Tables B-1 through B-7.

While SSA has made progress, its ERM is at the Emerging phase, the second of five, which is an early developmental level. At this level, SSA's risk management is not integrated, meaning SSA is managing risks in separate silos not collaboratively with a common understanding of risk across the Agency. We believe this limits SSA's ability to holistically identify, analyze, evaluate, respond to, and manage the risks it faces that could impede its mission and ability to serve its customers.²⁰

Implementation Plan Delays

SSA developed its first *ERM Implementation Plan* in FY 2020.²¹ The Plan projected ERM maturity by FY 2024. In FY 2022, SSA re-evaluated the Plan and adjusted its timeline, with maturity targeted for FY 2028.²² As of the date of our review, the activities in SSA's Plan that had not yet been implemented included the following:

- ERM training of its employees to provide them an understanding of ERM and its purpose. SSA is finalizing its initial training, which it plans to make available in FY 2024.²³ More in-depth training development is delayed until ERM is at a desired maturity phase.²⁴
- Assigning Risk Portfolio Managers who will be responsible to identify, assess, respond to, monitor, and report on sets of risks affecting their groups.²⁵
- Reporting channels to help keep those with ERM responsibilities informed with timely and relevant information throughout the implementation process and increase understanding of the ERM program and top risks affecting the Agency.

Per SSA, distribution and implementation of tools, templates, and processes developed to support ERM implementation required more time and review than originally anticipated. SSA reported it is approximately 1 year behind meeting implementation timeframes defined in its most recent *ERM Implementation Plan*.²⁶

²⁰ At the Emerging phase, *Circular A-123* does not require a comprehensive risk profile.

²¹ SSA, *Enterprise Risk Management Final Implementation Plan* (December 2019).

²² SSA reported it was impacted by several challenges over the last several years, including the pandemic, funding issues, and staffing losses.

²³ SSA did not specify when in FY 2024 the training would be made available as it depends on staffing resources needed to deliver the video.

²⁴ SSA calls its initial training ERM 101. The remaining trainings, ERM 102-ERM 107, will be developed or adjusted based on ERM 101's success and SSA needs. SSA initially planned to make these trainings available in phases between FYs 2022 through 2024.

²⁵ SSA stated, while it has been delayed in designating the individual role of Risk Portfolio Managers, the responsibilities have been carried out by other groups to help develop the risk profile.

²⁶ For more information about SSA's ERM implementation timeframes, see Appendix B, Table B-9.

Enterprise Risk Management Resources

SSA's ERM team consists of five SSA employees tasked with implementing and maturing ERM. According to the team, its ability to meet planned ERM milestones was impacted by competing non-ERM workloads, such as the *Federal Managers' Financial Integrity Act* Internal Control Program, Green Book compliance and other legally mandated priorities.²⁷

SSA engaged an outside contractor to support ERM implementation by creating several ERM plans and processes, paying the contractor approximately \$5.3 million for its work.²⁸ Since FY 2021, the contractor has created standard operating procedures, training and communication plans, a risk-analysis template, and additional templates to support separate programs collaborating to assess significant risk. Per SSA, it has not used many of the materials the contractor produced because of limited staffing resources, and it has not advanced to the ERM phases they were created to support.

In FY 2023, SSA awarded the contractor an additional contract for \$48,000 for advisory services, such as facilitating risk appetite discussions, coordinating, and combining cyber-security with ERM, and creating a structure to use its communication tool.²⁹

Enterprise Risk Management Governance

Circular A-123 encourages SSA to establish a governance structure for its risk-management function and suggests different ways oversight can be carried out, such as establishing a Risk Management Council, which may be combined with existing management groups to support ERM.³⁰ SSA established its ERMC in FY 2020. Since forming, the ERMC met infrequently, meeting only six times since it was established, and was not timely in its decision-making.³¹ For example, the ERMC did not decide on SSA's initial risk appetite, which is the broad amount of risk SSA is willing to accept in pursuit of its mission, until FY 2021; and it has not yet decided on all of its corresponding risk tolerance levels, which is the level of variance from its risk appetite that SSA is willing to accept in its performance.

With its delayed development of SSA's risk appetite and risk tolerance levels, the ERMC's efforts to promote a risk-aware culture throughout SSA has also been delayed. The ERMC has also yet to decide which components are responsible to manage SSA's different risk portfolios, a decision needed to help ensure risks are identified and communicated to facilitate understanding of the risks combined impact.

²⁷ *Circular A-123* does not stipulate resource requirements to implement an ERM capability. According to the Government Accountability Office, identifying a dedicated team to build and sustain the ERM function is a successful practice in managing risks. *Enterprise Risk Management, Selected Agencies' Experience Illustrate Good Practice in Managing Risk*, GAO-17-63, p. 15 (December 2016).

²⁸ SSA paid the contractor approximately \$5.3 million for work it performed FYs 2018 through 2023.

²⁹ As of August 2023, the contract was still in progress.

³⁰ *Circular A-123* identifies these risk-management functions as industry best practices. OMB, *Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, M-16-17*, part II, sec. A, p. 12 (July 15, 2016).

³¹ As of August 2023, the ERMC met six times between October 2020 and November 2022. Per the ERMC Charter, the members planned to meet periodically throughout the year, but not less than quarterly.

Risk Appetite and Tolerance Levels

Circular A-123 recommends ERM governance develop and implement core ERM policies and procedures, including a process to regularly ensure its risk appetite levels aligns with established risk tolerances and meet the organization's needs.³² While, in FY 2021, SSA's ERM governance structure developed its risk appetite, which established how much risk it is willing to accept. However, SSA has not established a process to regularly review, or assess when or under which circumstances it is willing to deviate from, its risk appetite (risk tolerance). We believe this approach limits SSA's ability to ensure its programs and operations are aligned with its risk appetite and any deviations from it within one silo of SSA's operations have been evaluated at the enterprise-level to understand the broader impact the deviations may have to SSA's ability to meet its mission.

After it developed its risk appetite in FY 2021, SSA did not re-evaluate it until FY 2023. Since FY 2023, SSA has changed leadership, which may have a different perspective on what SSA's risk appetite should be. Per SSA, in FY 2023, it worked with a contractor to update the risk-appetite statement and develop risk-appetite assessment tools to gradually align its risk appetite with risk tolerances, but those tools have not yet been put into use.³³ SSA reported it is re-evaluating its ERM governance structure, including changes to improve how it will carry out some of its governing functions and decision making.

Promoting Risk Awareness

Circular A-123 requires that agencies establish and foster a transparent culture that encourages people to discuss potential risks and other concerns with their superiors without fear of retaliation or blame. It also states the responsibilities of managing risks should be shared agency wide from the highest levels of leadership to the service delivery staff.³⁴ According to SSA, the ERMC helped promote risk awareness as SSA's way of doing business by creating, approving, and distributing its risk appetite in FY 2021. SSA indicated it distributed its risk appetite in its *Integrity Act Handbook* and on an Intranet webpage. SSA has future plans to use its *ERM Communications Plan* and trainings to help increase ERM awareness, which is critical to its success, but it has not implemented them to date.

³² *Circular A-123* identifies these risk management functions as industry best practices. OMB, *Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, M-16-17*, part II, sec. A, p. 12 (July 15, 2016).

³³ SSA stated the tools were developed and delivered as it completed updating its risk appetite statement. SSA plans to use the tools when it updates its risk appetite to reflect its new leadership's perspective.

³⁴ OMB, *Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, M-16-17*, p. ii and part II, sec. A, p. 12 (July 15, 2016).

RECOMMENDATIONS

We recommend SSA:

1. Make ERM implementation a priority by providing the ERM team the resources it needs to ensure ERM reaches maturity no later than the planned date of FY 2028, in accordance with its current *ERM Implementation Plan*.
2. Ensure as SSA is working toward reaching maturity that the ERMC is providing leadership over the ERM program and that key *Circular A-123* requirements are completed. For example, key requirements should include regular evaluation of SSA's risk appetite and risk tolerance levels and ERMC communications in support of an Agency-wide risk culture.

AGENCY COMMENTS

SSA agreed with our recommendations. The Agency's comments are included in Appendix D.

APPENDICES

Appendix A – SCOPE AND METHODOLOGY

To gain an understanding of Enterprise Risk Management (ERM) requirements and process, we:

- Reviewed Office of Management and Budget (OMB) *Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*,¹ to ensure compliance with all ERM requirements.
- Reviewed the *Enterprise Risk Management Practitioner's Guide for Offices of Inspectors General*, Council of the Inspectors General on Integrity and Efficiency (October 2019); *Inspectors General Guide to Assessing Enterprise Risk Management*, Council of the Inspectors General on Integrity and Efficiency (January 2020); *Standards for Internal Control in the Federal Government*, Government Accountability Office (September 2014); and Chief Financial Officers Council and the Performance Improvement Council, *Playbook: Enterprise Risk Management for the U.S. Federal Government* (July 2016).

To evaluate compliance and the extent of the Social Security Administration's (SSA) ERM implementation and maturity as of September 2023, we:

- Reviewed SSA's core team involved with SSA's planning and development of ERM.
- Reviewed SSA's initial (Fiscal Year [FY] 2018)) and revised (FY 2021) ERM frameworks and related Appendices.
- Reviewed SSA's initial and revised *ERM Implementation Plan* for FYs 2020 through 2024 and FYs 2023 through 2027, *ERM Communications Plan* as of February 2022, *ERM Training Plan* as of December 2021, *ERM Integration Framework* as of February 2021, *Maturity Model Evaluation* for FYs 2021, 2022, and 2023, and related documents to gain understanding of its ERM oversight, framework, implementation, and maturity.
- Reviewed task orders SSA awarded for ERM development, implementation, and/or ongoing management, including deliverables.

To evaluate SSA's ERM governance structure, we:

- Reviewed committee charters and meeting minutes.

To gain understanding of SSA's risk profile development and evaluate compliance, we:

- Reviewed SSA's Comprehensive Risk Register (FY 2017) for compilation of enterprise- and program-level risks identified by designated SSA staff.

¹ OMB, *Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*, M-16-17, and Attachment, OMB *Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*, M-16-17, part II, secs. A-C, pp.9 through 21 (2016).

- Reviewed SSA’s Risk Profile for FYs 2017 through 2020, and 2022 to determine changes to risks.

We conducted our review between January and December 2023. The information in this report includes publicly reported and internal planning materials. We relied on the documentation provided by the Deputy Commissioner for Budget, Finance, and Management related to its implementation, and maturation of ERM. We determined the information used in this report were sufficiently reliable given our audit objectives and intended use of the information. The principal entity reviewed was the Office of Budget, Finance, and Management.

We assessed the significance of internal controls necessary to satisfy the audit objective. This included an assessment of the five internal control components, including control environment, risk assessment, control activities, information and communication, and monitoring. In addition, we reviewed the principles of internal controls as associated with the audit objective. We identified the following components and principles as significant to the audit objective:

- Component 1: Control Environment
 - Principle 1 – Demonstrate commitment to integrity and ethical values
 - Principle 2 – Exercise oversight responsibility
 - Principle 3 – Establish structure, responsibility, and authority
 - Principle 4 – Demonstrate commitment to competence
- Component 2: Risk Assessment
 - Principle 6 – Define objectives and risk tolerances
 - Principle 7 – Identify, analyze, and respond to risk
 - Principle 8 – Assess fraud risk
- Component 3: Control Activities
 - Principle 12 - Implement control activities
- Component 4: Information and Communication
 - Principle 13 – Use quality information
 - Principle 14 – Communicate internally
 - Principle 15 – Communicate externally
- Component 5: Monitoring
 - Principle 16 – Perform monitoring activities

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix B – ENTERPRISE RISK MANAGEMENT IMPLEMENTATION STRUCTURE

The Social Security Administration (SSA) developed an *Enterprise Risk Management (ERM) Implementation Plan* to help progress the Agency’s ERM implementation by building repeatable processes for risk management, developing a risk-aware culture, and integrating risk management as part of its goal of continuous improvement.¹ The ERM Implementation Plan outlines the goals, objectives, and strategies for SSA to properly integrate ERM Agency-wide in a 5-Fiscal Year (FY) period. SSA’s ERM implementation structure includes 7 task areas aligned with 80 comprehensive key activities as defined in its Maturity Model Evaluation (Tables B-1 through B-7),² to be implemented in 4 phases (Table B-8), across 4 periods (Table B-9) to fully implement and mature its ERM. SSA developed a Maturity Evaluation Model to annually self-assess its level of ERM implementation and maturity progress.

The foundational elements of an ERM Framework establish the backbone for SSA’s ERM roles, responsibilities, and procedures and the guiding principles upon which the program will be built. These activities focus on identifying and refining the basic principles that will drive SSA’s future ERM Program. SSA scored its progress as having 8 of its 23 foundational elements activities present in FY 2023.

Table B–1: Foundational Element Activities

Count	Description of Foundation Element Activities	Score as of FY 2023
1	Adequate resources have been dedicated to support the ERM function.	0
2	Agency ERM stakeholders have a clear understanding of the ERM objectives relative to traditional approaches to risk management, and the role of ERM as a strategic tool for managing enterprise-level risks.	0
3	The Agency has defined and widely communicated to managers and ERM stakeholders what it means by the term risk.	0
4	The Agency has developed and documented an ERM Framework to drive the development and execution of policies and procedures to support the maturation of the ERM program.	1
5	The Agency has explicitly assigned enterprise-wide risk management authority and responsibility to a senior executive (that is, the Deputy Commissioner [DC] for Budget, Finance, and Management) and a senior executive committee (the Enterprise Risk Management Council (ERMC) (for example, identified an internal risk champion or risk management leader).	1
6	ERM stakeholders involved in the implementation and maturity of the ERM program have effective risk management capabilities and competencies.	0
7	Senior executives regard ERM as an ongoing process rather than just a project.	1

¹ SSA’s ERM Implementation Plan for FYs 2023-2027, as of July 2022. The most recent version as of FY 2023.

² Each Task Area includes specific activities, one score for each executed activity (that is, Foundational Elements includes 23 specific activities for a possible total score of 23). The total score for each Task Area is combined to determine overall maturity level, which a maximum score of 80 indicating maturity, Advanced level 5. For more information about the Maturity Evaluation score range, see Appendix C.

Count	Description of Foundation Element Activities	Score as of FY 2023
8	Both the Commissioner and Agency Senior Executives view ERM as an ongoing process that will continually evolve over time.	0
9	The Commissioner embraces the need and provides adequate endorsement of an enterprise-wide approach to risk oversight that seeks to obtain a top-down view of major risk exposures.	0
10	The Senior Executive with explicit responsibilities for enterprise-wide risk management leadership (that is, the DC) is a direct report of the Commissioner (or a senior executive risk committee is used to provide that leadership and the committee chair reports to the Commissioner (that is, the ERM)).	1
11	Enterprise-wide risk management principles and guidelines have been identified and defined by executive management and have been formally communicated to all business units.	0
12	The Agency has expressed in writing its overall appetite for risk taking.	1
13	The Agency has used at least some quantitative measures in defining its risk appetite.	0
14	The Agency has defined its appetite for risks within the internal, external, and strategic risk categories.	1
15	ERM stakeholders, including the Office of Financial Policy and Integrity, the ERM, and the DC or Assistant DC for each component, are aware of the Agency's overall appetite for risk taking.	1
16	The Commissioner and ERM has concurred with the Agency's risk appetite.	0
17	ERM stakeholders reassess the risk appetite on an annual basis to identify necessary revisions.	0
18	The Agency identifies Key Performance Indicators (KPI) and Key Risk Indicators (KRI) to monitor performance and significant risk areas.	0
19	The Agency assigns responsibility of KPIs and KRIs to specific ERM stakeholders for monitoring and reporting purposes.	0
20	Agency executives and ERM stakeholders have identified thresholds or trigger points whereby risk metrics indicate that an emerging risk warrants greater management and/or Commissioner attention.	0
21	Each member of the Senior Executives team and Agency ERM stakeholders have provided input into the risk identification process.	1
22	ERM stakeholders have established a process to compile risk information within defined risk categories (internal, external, strategic) from across the Agency to create an aggregate inventory of enterprise-wide risks.	0
23	The ERM promotes discussion on the most significant enterprise risks through scheduled periodic and ad hoc discussions.	0
Total Score for Foundational Elements Activities		8

The risk assessment process attempts to promote the analysis of risks from both a top-down and bottom-up position to allow SSA to evaluate and review a portfolio of risk that represents insight into all areas of Agency exposure. Through established risk assessment procedures, SSA executives are afforded the ability to increase the chance of experiencing fewer unanticipated outcomes and executing a better assessment of risk associated with changes in the environment. SSA scored its progress as having 2 of its 15 risk assessment activities present in FY 2023.

Table B-2: Risk Assessment Activities

Count	Description of Risk Assessment Activities	Score as of FY 2023
1	Risks have been described in terms of events that would affect the achievement of goals, rather than simply a failure to meet goals (that is, risks can have both positive and negative aspects to the Agency).	0
2	The Agency developed metrics and guidelines to consistently consider the likelihood and impact of identified risks across programmatic areas and risk management processes.	0
3	The Agency considers factors outside of likelihood and impact (for example, risk persistence, root cause analysis, etc.) to facilitate ranking and prioritization of identified risks.	0
4	The Agency uses standardized tools and templates to document risk identification, assessment, and response information.	0
5	The Agency has defined the period in which risks should be assessed (for example, annually, triennially, etc.) in the SSA ERM Framework and a methodology for assessing and scoring the likelihood and impact of identified risks.	1
6	SSA's ERM promotes consideration of risks with low probability but high impact (for example, black swan, tail events).	0
7	Senior Executives and ERM stakeholders are aware of the results of risk assessments, and the Agency's portfolio of risks to identify similar threat sources or events to provide concurrence on the results and conclusions.	0
8	Each year, the Agency assesses risk responses to determine the effectiveness of the existing response, if modifications are necessary, and identify potential duplicative efforts and streamlining opportunities.	0
9	The Agency has documented responses for risks outside of the most significant (that is, top 8-12 risks), identified risk owners, and objectively assesses the effectiveness of the existing risk responses.	0
10	Senior Executives and ERM stakeholders have reached a consensus on the most significant risks (that is, top 8-12 risks) and documented them within a Risk Profile.	1
11	The Agency has documented responses to its most significant risks (that is, top 8-12 risks), identified risk owners, and objectively assesses the effectiveness of the existing risk responses.	0
12	The Agency leverages standardized procedures to identify and assess the most significant risks (that is, top 8-12 risks) at least annually.	0
13	The Agency compiles input and feedback from various levels of the Agency (for example, Senior Executives, Oversight Bodies, Programmatic and Component leads, etc.) on the risk identification and assessment process.	0
14	Senior Executives and ERM stakeholders have provided independent assessments of both significant risks (that is, top 8-12 risks) and other risks that warrant monitoring.	0
15	The Agency has developed and monitors key risk indicators that are lagging in nature (that is, metrics that show when risk events have occurred or are escalating).	0
Total for Risk Assessment Activities		2

SSA has numerous methods and processes for identifying and managing risk, monitoring performance, and reporting results such as strategic planning, performance management, and its *Federal Managers' Financial Integrity Act* Internal Control Program. The integration area seeks to consolidate these separate processes and methods into a defined hierarchy to support the Agency's ERM effort. SSA scored its progress as having 4 of its 15 integration activities present in FY 2023.

Table B–3: Integration Activities

Count	Description of Integration Activities	Score as of FY 2023
1	The Agency has identified integration points (for example, existing review programs and assessments) for consolidation within the ERM Framework.	1
2	The Agency has established mechanisms for communication across integration points (for example, integration contacts, touchpoints, understanding meetings, etc.).	0
3	The Agency has determined how the reporting requirements in integration points can support ERM outputs (for example, Risk Profile).	0
4	The Agency has developed standardized tools and templates to collect integrated risk information sources.	1
5	SSA ERM stakeholders link risks identified by the ERM process to strategic goals in its strategic plan to evaluate the impact of those risks on the strategic success of the Agency.	0
6	Agency executives link the top risk exposures to strategic objectives to determine which objectives face the greatest number of risks and to determine which risks impact the greatest number of objectives.	0
7	When evaluating a range of strategic options, SSA considers the potential impact of each option on its existing enterprise-wide risk profile.	0
8	The Senior Executive with explicit responsibility for the ERM program (or the chair of the committee with that responsibility) (that is, the DC and ERMC) are actively engaged in the strategic planning process.	1
9	The Agency's risk appetite statement guides the strategic planning process (that is, if it has an adverse risk appetite, risk avoidance is a core objective).	0
10	The Agency's risk appetite is applied to integration points as applicable, to ensure a consistent approach to managing risk is used.	0
11	The Agency's existing Risk Profile (that is, output from the ERM processes) is an important input for the strategic planning process.	0
12	The Agency's Executive Assurance Process purpose, timeline, and reporting processes have been revised to support ERM objectives.	1
13	The Agency has aligned the Strategic Objective Review with ERM objectives and timelines to support development of the Risk Profiles and other ERM initiatives.	0
14	The Agency leverages tools, techniques, and templates from the Fraud Risk Management Framework to support development of the Risk Profiles and other ERM initiatives.	0
15	The Agency leverages tools, techniques, and templates from the Cyber Security Framework to support development of the Risk Profiles and other ERM initiatives.	0
Total for Integration Activities		4

Training is a fundamental element of SSA’s ERM Program. Effective training sessions raise stakeholder awareness, engages employees from all Agency levels, and aids in the maturation of the ERM Program. To ensure the ERM Program continues maturing and evolving, SSA must ensure all pertinent Agency stakeholders have the relevant knowledge and skills to carry out the activities of its ERM Program. SSA scored its progress as having two of its six training activities present in FY 2023.

Table B–4: Training Activities

Count	Description of Training Activities	Score as of FY 2023
1	Senior Executives and ERM stakeholders routinely evaluate the existing knowledge of individuals with ERM responsibilities, such as internal control oversight bodies (for example, Senior Assessment Team, ERM Council, Executive Internal Control Committee, National Anti-Fraud Council, etc.).	0
2	The Agency has assessed of training needs for the various levels of ERM stakeholders.	1
3	Training for various levels of the Agency and other ERM stakeholders has been developed using the results of the needs assessment.	0
4	The Agency has developed a documented training plan based on the results of the training needs assessment that includes the training developed, delivery method, schedule, and other supporting information (for example, objective, frequency, audience, etc.).	1
5	Trainings are delivered to various ERM stakeholder groups in an approach that promotes flexibility and the opportunity to proactively modify training content.	0
6	ERM Training program and Training Plan are periodically reviewed to determine effectiveness, potential gaps, and identify potential revisions.	0
Total for Training Activities		2

Deploying a technology solution is a logical step in the maturation of an ERM Program. A comprehensive technology solution selected to meet the SSA’s ERM Program requirements provides added efficiencies, linkages between processes, facilitate clear communication channels, and brings credibility to its ERM Program. A technology solution also supports integration with existing risk data and monitoring of business processes, program-level, and enterprise-wide risks into one solution for added transparency over the Agency’s portfolio of risks. SSA scored its progress as having two of its four technology solution activities present in FY 2023.

Table B–5: Technology Solution Activities

Count	Description of Technology Solution Activities	Score as of FY 2023
1	Senior Executives and ERM stakeholders have established detailed technology requirements to align related acquisitions to the current and long-term objectives of the ERM program.	1
2	The Agency has selected a vendor for ERM technology solutions that align with the requirements identified by Senior Executives and ERM stakeholders.	1
3	The Agency has documented an implementation plan for ERM technology solutions acquired to support the program, including trainings needed for target users, Standard Operating Procedures, and any related tools and templates.	0
4	Senior Executives and ERM stakeholders annually assess the Standard Operating Procedures, tools, and templates utilized in support of the technology solution to ensure continued relevance.	0
Total Score for Technology Solution Activities		2

A well-documented communication plan is used to clarify SSA’s communication goals and objectives, establish stakeholder’s roles and responsibilities and tools, as well as identify methods to facilitate Agency communication. SSA’s Communication Plan seeks to document the strategy for communicating between key stakeholders throughout ERM implementation and in day-to-day risk management activities. SSA scored its progress as having one of its eight communication and reporting activities present in FY 2023.

Table B–6: Communication and Reporting Activities

Count	Description of Communication and Reporting Activities	Score as of FY 2023
1	The Agency has established mechanisms for communicating and reporting results across ERM stakeholder groups and facilitate change through feedback among ERM participants (for example, ERMC, Senior Executives, etc.) via a documented communication plan.	0
2	Reporting mechanisms align or consider integration points (Executive Assurance Process templates) and ERM reporting requirements and output deadlines (for example, Risk Profiles).	0
3	The Agency has developed roles and responsibilities for communicating aspects of the ERM program (for example, Mission Statement, KPIs, KRIs, Executive messages, etc.) and designated specific personnel to act in these communication roles.	0
4	The Agency has documented a schedule for communicating across ERM stakeholder groups and identified the required personnel and points of contact.	0
5	The Agency leverages reporting mechanisms within integration points (for example, <i>Agency Strategic Plan</i> , <i>Annual Performance Report</i> , <i>Agency Financial Report</i>) to disseminate relevant ERM information to internal and external Agency stakeholders.	0
6	The DC and/or ERMC regularly receives and reviews dashboards or other report that provides the status of key risks and/or risk response plans at the enterprise and portfolio levels through KPIs and KRIs.	0

Count	Description of Communication and Reporting Activities	Score as of FY 2023
7	Office of Financial Policy and Integrity executives have formally presented an overview to the Commissioner and DC about the Agency's processes that represent its approach to ERM.	1
8	The Agency periodically documents potential improvements and ERM best practices through lessons learned, with results disseminated to Senior Executives and ERM stakeholders.	0
Total for Communication and Reporting Activities		1

Conducting ongoing evaluations over SSA's efforts to maximize the value achieved during ERM implementation will help provide it with a clear-eyed view of the strengths and weaknesses of the program as well as opportunities available for moving toward the next level of ERM Maturity. Additionally, assessing SSA's maturation on its Maturity Model assists the Agency in confirming it has successfully implemented the various facets of a successful ERM Program. SSA scored its progress as having two of its nine evaluation and maturity activities present in FY 2023.

Table B-7: Evaluation and Maturity Activities

Count	Description of Evaluation and Maturity Activities	Score as of FY 2023
1	The Agency develops criteria and metrics for determining the effectiveness of ERM practices and a process for developing and implementing updates to the ERM program.	0
2	The Agency obtains an annual objective assessment of its ERM processes periodically (that is, through internal audit or third party ERM expert evaluations) to determine alignment between ERM goals and objectives and the ERM Maturity Model.	1
3	The Agency has developed a mechanism or tool for reporting the progress of the ERM program against the <i>ERM Implementation Plan</i> on a quarterly basis	0
4	Output from the Agency's ERM processes about significant risk exposures function as an input to public reporting mechanisms and mediums (for example, press releases, <i>Agency Financial Report</i> , <i>Annual Performance Report</i> , etc.) to inform other internal and external Agency stakeholders	0
5	The Agency's ERM processes encourage the consideration of opportunities where it can take informed risks to generate incremental returns.	0
6	Senior executives seek to understand and monitor emerging ERM best practices.	0
7	The ERM process encourages monitoring on a regular basis (more than once a year) any events substantially impacting the assessments of likelihood and impact.	0
8	The Agency evaluates risk events that have occurred to better understand why the risk occurred and whether there were failures in the Agency's ERM processes.	0
9	The Agency identifies and subsequently implements changes to improve its ERM processes.	1
Total Score for Evaluation and Maturity Activities		2

Within each task area, SSA further defined its *ERM Implementation Plan* into four key phases.

Table B–8: ERM Implementation Phases

Phase	Phase Category	Phase Description
1	Planning	Strategizing and planning implementation efforts including strategy-setting meetings, brainstorming sessions, adaptation of lessons learned, and other necessary activities to define implementation activities.
2	Design and Development	Efforts to design and develop the supporting structure for ERM (that is, policy and procedural documents, evaluation metrics, integration points, and reporting mechanisms).
3	Implementation	Efforts to implement and execute the policies and procedures developed as part of the ERM Framework.
4	Maturity	Efforts to support goal of continuous improvement of ERM Framework and supporting processes and tools. Evaluation of progress on ERM advancement across the Agency and adjust ERM implementation as necessary to adjust gaps in meeting desired maturity state.

To complete the task areas and ensure it was on track with its maturity plan, SSA estimated timeframes for each phase of the *ERM Implementation Plan* that includes action items.³

Table B–9: ERM Implementation Timeframes

Timeframe	Description
Now	Action items with an estimated time of completion of within 1 year.
Next	Action items with an estimated completion time greater than 1 year but less than 3 years.
Later	Action items with an estimated completion time of greater than 3 years. Such items generally represent advanced maturity level and focus of continuous improvement of previously completed items.
Recurring	Actions items designed to foster continuous improvement to ensure previously developed ERM resources remain relevant and retain usefulness.

Note: ERM Implementation timeframes are based on SSA's *ERM Implementation Plan* as of July 2022.

³ SSA did not assign action items to certain task areas with consideration of previous progress and anticipated resource constraints.

Appendix C – MATURITY EVALUATION SCORE RANGE

The Social Security Administration's (SSA) Maturity Model has five distinct levels and phases, ranging from 1, Initial phase with the lowest maturity, to 5, Advanced phase with the highest maturity. At the Advanced level, a mature ERM embeds discussions of risks in the Agency's planning, resource management, and decision making; and the Agency has early warning systems to alert management when risks exceed established thresholds. Each level is based on the total score of SSA's execution of its fundamental activities relative to its task areas: Foundational Elements, Risk Assessment Activities, Integration, Training, Technology Solution, Communication and Reporting, and Evaluation and Maturity.¹

Table C–1: SSA Maturity Model Levels and Score Range

Maturity Level	Maturity Phase	Phase Description	Maturity Evaluation Score Range
1	Initial	<ul style="list-style-type: none"> No formal or documented program Risks are addressed as they arise No standardized tools or techniques 	0 to 5
2	Emerging	<ul style="list-style-type: none"> Limited alignment of risk to strategy Risk management process formalization is ongoing Risk is managed in silos 	6 to 33
3	Integrated/ Defined	<ul style="list-style-type: none"> Full risk management framework established policies and procedures defined Risks align with strategy Common tools and techniques are used 	34 to 56
4	Predictive	<ul style="list-style-type: none"> ERM is recognized and established across the organization The use of risk management tools and techniques is standardized Risk management and internal controls are integrated 	57 to 69
5	Advanced	<ul style="list-style-type: none"> Discussions of risks embedded in strategic planning, resource allocation, policy, and other key decisions Technology is utilized Early warning systems are used to identify risks above established thresholds 	70 to 80

¹ For more information about SSA's Task Areas, see (Tables B-1 through B-7).

Appendix D – AGENCY COMMENTS



SOCIAL SECURITY

MEMORANDUM

Date: July 8, 2024

Refer To: TQA-1

To: Michelle L. H. Anderson
Acting Inspector General

From: Dustin Brown 
Acting Chief of Staff

Subject: Office of the Inspector General Draft Report "The Social Security Administration's Enterprise Risk Management" (022323) – INFORMATION

Thank you for the opportunity to review the draft report. We agree with the recommendations.

Please let me know if I can be of further assistance. You may direct staff inquiries to Hank Amato at (407) 765-9774.



- Mission:** The Social Security Office of the Inspector General (OIG) serves the public through independent oversight of SSA's programs and operations.
- Report:** Social Security-related scams and Social Security fraud, waste, abuse, and mismanagement, at oig.ssa.gov/report.
- Connect:** [OIG.SSA.GOV](https://oig.ssa.gov)


Visit our website to read about our audits, investigations, fraud alerts, news releases, whistleblower protection information, and more.

Follow us on social media via these external links:

 @TheSSAOIG

 OIGSSA

 TheSSAOIG

 Subscribe to email updates on our website.