# 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.