NCUA
National Credit Union Administration

Office of Inspector General

OIG-26-05

Audit of the NCUA's Enterprise Risk Management Risk Profiles

May 20, 2026

NCUA

OFFICE OF INSPECTOR GENERAL

Memorandum

SENT BY EMAIL

DATE: May 20, 2026

TO: Distribution List

FROM: Acting Deputy Inspector General Annie Golden
Office of Inspector General

SUBJECT: Audit of NCUA's Enterprise Risk Management Risk Profiles

The National Credit Union Administration (NCUA) Office of Inspector General (OIG) conducted this self-initiated audit to assess the NCUA's Enterprise Risk Management Risk Profiles. The objective of our audit was to determine if the NCUA adequately established, maintained, and used risk profiles to address enterprise-level risks.

Our audit determined the NCUA's Enterprise Risk Management Council (ERM Council) did not consistently establish, update, or use risk profiles to address the agency's enterprise-level risks. The NCUA's ERM Council needs to improve the regular assessment and updating of all enterprise-level risks. The ERM Council should also improve how it communicates its results to necessary agency officials, as appropriate. Without improvements, the NCUA may not consistently make informed decisions to enable proactive mitigation and monitoring strategies of enterprise-level risks so as not to exceed the agency's risk appetite. We are making two recommendations in our report and note that NCUA management plans to take corrective action to address the issues we identified.

We appreciate the cooperation and courtesies NCUA management and staff provided to us during the audit. If you have any questions on the report or its recommendations, please contact me at 703-518-6350.

Distribution List:
Chairman Kyle S. Hauptman
Executive Director Larry Fazio
Chief of Staff Sarah Bang
Acting Deputy Executive Director Kelly Lay
General Counsel Frank Kressman
OEAC Director Sierra Robinson
Acting Chief Financial Officer Melissa Lowden

Table of Contents

Executive Summary

OIG-26-05 Audit of the NCUA's Enterprise Risk Management Risk Profiles

Why We Did This Audit

The NCUA OIG conducted this self-initiated audit to assess the NCUA's Enterprise Risk Management Risk Profiles. The objective of our audit was to determine if the NCUA adequately established, maintained, and used risk profiles to address enterprise-level risks. The scope of our audit covered the NCUA's risk profiles from January 1, 2023, to April 1, 2025.

Office of Management and Budget (OMB) Circular A-123 (2016) [1] required "an effective agency-wide approach to addressing the full spectrum of the organization's significant risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos." The primary purpose of a risk profile is to provide an analysis of the risks an agency faces toward achieving its strategic objectives arising from its activities and operations, and to identify appropriate options for addressing significant risks. In 2026, the Office of Management and Budget reissued Circular A-123, which revised the requirement of risk profiles to a best practice.

What We Found

Our audit determined the NCUA's Enterprise Risk Management Council (ERM Council) did not consistently establish, update, or use risk profiles to address the agency's enterprise-level risks. The NCUA's ERM Council needs to improve the regular assessment and updating of all enterprise-level risks. The ERM Council should improve how it communicates its results to necessary agency officials, as appropriate. Without improvements, the NCUA may not consistently make informed decisions to enable proactive mitigation and monitoring strategies of enterprise-level risks so as not to exceed the agency's risk appetite.

What We Recommend

We are making two recommendations in our report to address the issues we identified.

1. Implement a regular assessment and briefing of all enterprise-level risks, such as through discussion of risk profiles at ERM Council meetings, on a frequency commensurate with risk exposure to monitor that each risk is managed within risk appetite.

2. Clarify how the ERM Council should communicate risk results to agency officials who implement decisions.

[1] OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, M-16-17 (2016), was in effect during the audit scope period of January 1, 2023, to April 1, 2025. OMB issued a revised A-123 on March 10, 2026.

Background

The NCUA is an independent federal agency that insures deposits at federally insured credit unions and charters and regulates federal credit unions. The NCUA protects the safety and soundness of the credit union system by identifying, monitoring, and managing risks to the Share Insurance Fund (SIF), which provides up to $250,000 of federal share insurance to millions of accounts in all federally insured credit unions. The agency operates a headquarters in Alexandria, Virginia; an Asset Management and Assistance Center (AMAC) in Austin, Texas to liquidate credit unions and recover assets; and three regional offices that carry out the agency's supervision and examination program, along with the Office of National Examinations and Supervision (ONES). The NCUA is responsible for the regulation and supervision of 4,331 federally insured credit unions with more than $2.4 trillion in assets across the United States and its territories as of September 30, 2025.

Enterprise Risk Management (ERM)

As defined by OMB Circular A-123 (2016),[2] ERM is an effective agency-wide approach to addressing the full spectrum of an agency'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 into how to effectively prioritize resource allocations to ensure successful mission delivery. Although 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.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO)[3] defines ERM as "the culture, capabilities, and practices, integrated with strategy-setting and its performance, that organizations rely on to manage risk in creating, preserving, and realizing value." The COSO ERM framework is comprised of five interrelated components: governance and culture; strategy and objective setting; performance; review and revision; and information, communication, and reporting. Although connected to internal controls, ERM is more closely aligned with strategy with a focus on creating, preserving, and realizing value.

The five components in the framework are comprised of 20 principles.

[2] OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, M-16-17 (2016), was in effect during the audit scope period of January 1, 2023, to April 1, 2025. OMB issued a revised A-123 on March 10, 2026.

[3] COSO is a private sector initiative jointly sponsored and funded by the American Accounting Association (AAA), American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), Institute of Management Accountants (IMA), and the Institute of Internal Auditors (IIA).

Figure 1: COSO ERM Components and Framework

Source: COSO Enterprise Risk Management—Integrating with Strategy and Performance

OMB A-123 Guidance

OMB Circular A-123 (2016) guided executive agencies on the design and implementation of ERM capabilities and practices, including the establishment of agency-level risk appetite. It outlined the following required ERM activities:

- Governance
- Risk Profiles
- Implementation

On March 10, 2026, OMB issued a revised A-123 that provides streamlined guidance to improve internal control assessment and continuous monitoring. While the revised circular no longer mandates risk profiles, the guidance identifies the development of a risk management council, the implementation of ERM practices, and the creation of a risk profile as best practices.

Governance

Agency governance should include a process that considers the following characteristics identified in industry best practices:

- Developing and implementing core policies and procedures with respect to ERM, including a process to define risk appetite and establish risk tolerance thresholds,
- Ensuring the current risk levels and processes are consistent with the established risk tolerance thresholds and policies,
- Supporting implementation of effective controls,
- Developing strong reporting systems and analysis that incorporate quantitative and qualitative information to provide effective portfolio views of risk,
- Identifying emerging risks, concentrations of risk, and other situations that could be properly assessed, and
- Elevating critical issues to appropriate levels within an agency in a timely fashion.

Risk Profiles

Agencies must maintain a risk profile. The primary purpose of a risk profile is to provide an analysis of the risks an agency faces toward achieving its strategic objectives arising from its activities and operations, and to identify appropriate options for addressing significant risks. The risk profile assists in facilitating a determination around the aggregate level and types of risk that the agency and its management are willing to assume to achieve its strategic objectives.

Agencies have discretion in terms of the appropriate content and format for their risk profiles, but risk profiles should include the following seven components:

- Identification of Objectives – Specific strategic, operations, reporting, and compliance objectives must be identified and documented to facilitate identifying risks in these areas.
- Identification of Risk – Risks should be initially identified by using a structured and systematic approach to recognize where the potential for undesired outcomes or opportunities can arise. Once initial risks are identified, it is important to re-examine risks on a regular basis to identify new risks or changes to existing risks.
- Inherent Risk Assessment – OMB Circular A-123 defines inherent risk as the exposure arising from a specific risk before any action has been taken to manage it beyond normal operations. Inherent risks should be ranked by appropriate categories, based on the impact and likelihood that each risk might occur.
- Current Risk Response – Risk response (the action taken to manage the risk) may involve risk acceptance, avoidance, reduction, or sharing. Formulation of risk responses should consider the agency's risk appetite and risk tolerance thresholds.
- Residual Risk Assessment – The residual risk assessment involves identifying the exposure remaining from an inherent risk after action has been taken to manage it, and ranking the residual risk by category, based on the impact and likelihood that each risk might occur and using the same assessment standards as the inherent risk assessment.
- Proposed Action – Proposed actions are any additional actions taken to further reduce the exposure of residual risk.
- Proposed Risk Response Category – Responsible officials should identify existing management processes to implement and monitor proposed actions.

Implementation

The management of risk must be regularly reviewed to monitor whether the risk profile has changed and to determine if risk management is effective or if further action is necessary. At least annually, agencies should determine whether risk profiles have changed, update

risk profiles as needed, and assess all aspects of the risk management process. In addition, agencies must integrate ERM processes with existing strategic reviews and internal control processes required by Government Performance and Results Act Modernization Act of 2010 (GPRA Modernization Act) and Federal Managers Financial Integrity Act of 1982 (FMFIA).[4]

NCUA's Approach to ERM

The NCUA is exposed to a variety of risks that relate to its objectives, strategies, operations, reputation, and environment. Through the NCUA's ERM program, the agency expects to manage risks to achieve its mission and maximize opportunities across the agency. ERM addresses the full spectrum of risks related to achieving the NCUA's strategic objectives and delivers agency leadership a portfolio view of risk to help inform decision-making.

In May 2015, NCUA identified the need for an ERM program to identify, assess, prioritize, respond to, and monitor risks and opportunities at an enterprise level. The ERM Council was formally established by the Executive Director on October 2, 2015, and since that time has been focused on building the ERM foundation, identifying, assessing, and prioritizing enterprise-level risks, and developing risk response plans for those risks.

The NCUA ERM charter[5] assigns the ERM Council with primary oversight of ERM and the risk function. The ERM Council is responsible for independently assessing enterprise risks and ensuring sound policies, procedures, and practices are in place for enterprise-wide management of NCUA's enterprise-level risks. The ERM Council is comprised of the Deputy Executive Director, who is the Chair; Chief Financial Officer (CFO); Chief Information Officer (CIO); Chief Economist; Director of Examination and Insurance (E&I); Director of Office of Continuity and Security Management (OCSM); Director of Office of Business Innovation (OBI); and no fewer than two additional senior roles to rotate at the Chair's discretion, of which not less than one shall be selected from the Regional Directors or the Director of the Office of National Examinations and Supervision, and not less than one shall be selected from Central Office Directors not otherwise specified. ERM Council meetings should take place at least quarterly. The Office of the Chief Financial Officer (OCFO) should retain documentation of the assessment process, procedures, and annual results for at least 3 years.

The charter provides:

[4] For CFO Act agencies, OMB Circular A-123 (2016) required annual reporting of agency risk profiles to OMB. Because the NCUA is not a CFO Act agency, it was not required to report risk profiles to OMB.

[5] The NCUA ERM charter in place during the scope of the audit (January 1, 2023, to April 1, 2025) stated that it was effective April 11, 2019, and was signed January 10, 2020. During fieldwork, a new NCUA ERM charter was established effective August 14, 2025. The most significant change in the new charter is the ERM Council's composition, which is the Deputy Executive Director (Chairperson), four Central Office executives, and one executive from each of the three Regions and ONES. This audit did not assess the changes to the charter.

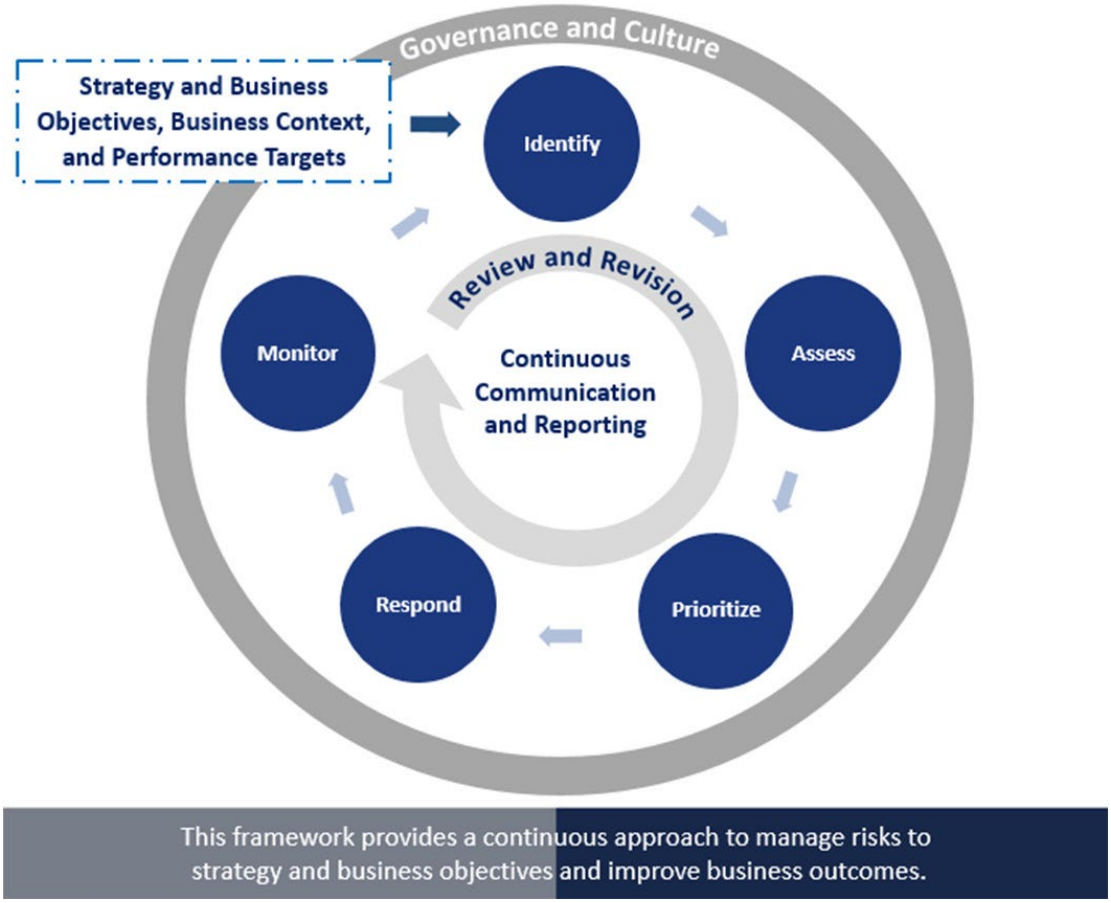
> The Council's mission is to optimize risk management prioritization and mitigation decisions to minimize the risks that events adversely impact the successful achievement of the NCUA's strategic goals and objectives. The Council seeks to establish a risk aware culture and appropriate risk management throughout the NCUA by clarifying roles and responsibilities and elevating the importance of proper risk management as function of all roles within the NCUA…The NCUA management is responsible for establishing processes to identify and manage risks on an ongoing basis. The Council will collaborate with NCUA management to assign and monitor corrective action plans identified by internal and external assessments, reviews, audits, and evaluations. The Council enables executive level monitoring of the review process and actions taken to mitigate risks identified.

Responsibilities of the Council include:

- Acting as an advocate for risk conversations and promoting a risk-aware culture at NCUA.
- Defining, establishing, and supporting a continuous ERM framework (including policies, procedures, and practices) that facilitates the identification, assessment, prioritization, response to and monitoring of risk at the enterprise level.
- Establishing the risk appetite for each category of risk within the context of the NCUA Board's risk management philosophy.
- Considering any changes to the business context that may impact the NCUA's strategy or risk appetite and its link to new, emerging, or manifesting risks.
- Establishing and maintaining a risk profile for all identified enterprise-level risks, including consistent methods to prioritize, respond to, and monitor enterprise-level risks.
- Ensuring actions taken to address risks and pursue opportunities align with the agency's strategy and risk appetite, optimize the agency's decision-making and performance, and consider resource availability or limitations.
- Reviewing and discussing with the NCUA Board and Executive Director on an ongoing basis, and the Inspector General when warranted, any significant risks or exposures and the agency's management of risks, culture, and performance.

The NCUA established the following framework for enterprise risk management to consistently evaluate risks across the NCUA through an established ERM process. The NCUA's ERM objectives are to integrate and improve decision-making to aid in achievement of the agency's mission and strategic goals, communicate the amount of risk the agency is willing to accept in pursuit of strategic goals and objectives through risk appetite statements, consistently evaluate risks across NCUA through an establish ERM process (as identified in Figure 2), and stay apprised of emerging and manifesting risks.

Figure 2: NCUA ERM Framework



NCUA developed the enterprise risk appetite statement, which defines senior leadership's overarching risk management philosophy. In NCUA's Strategic Plan (2022-2026), the NCUA stated the following regarding risk appetite:

> The NCUA is vigilant and has an overall judicious risk appetite. The NCUA's primary goal is to ensure the safety and soundness of the nation's credit union system and the agency recognizes it is not desirable or practical to avoid all risk. Acceptance of some risk is often necessary to foster innovation and agility. This risk appetite will guide the NCUA's actions to achieve its strategic objectives in support of providing, through regulation and supervision, a safe and sound credit union system, which promotes confidence in the national system of cooperative credit.

NCUA's risk appetite statement is linked to NCUA's overall risk management approach outlined in Figure 2 above.

In early 2022, NCUA used its 2017 risk appetite statement and benchmarked the risk statements from other federal agencies to refresh its risk appetite statement. The ERM

Council then took the following three actions, which led to a revised risk appetite framework:

- Reviewed and updated the risk categories and their definitions.
- Identified common agency activities aligned to each category.
- Assigned risk appetites for each activity.

The risk appetite framework includes the following risk categories:

1. Technology and Information Management Risk
2. Supervision Risks
3. Human Capital Risk
4. Legal and Regulatory Compliance Risk
5. Operational Risk
6. Governance and Strategic Risk
7. Financial Management Risk
8. External Risk

For each risk category, the NCUA identified associated activities to carry out. The agency defined whether it has an averse, moderate, or tolerant appetite for risks that could impact activities.

In 2021, in coordination with the update of the agency's risk appetite statement, the ERM Council reviewed the agency's inventory of identified risks. At the conclusion of its review, the ERM Council adopted an inventory of seven enterprise-level risks and six risks it considered "Of Concern" to the agency.

The ERM Council identified seven risks that were elevated to the enterprise level (enterprise-level risks).

Table 1: Enterprise-Level Risk, Risk Category, and Associated Risk Statement

Enterprise-Level Risk	Risk Category	Risk Statement
(b) (2), (b) (5), (b) (8)	(b) (2), (b) (5), (b) (8)	(b) (2), (b) (5), (b) (8)
(b) (2), (b) (5), (b) (8)	(b) (2), (b) (5), (b) (8)	(b) (2), (b) (5), (b) (8)

		(b) (2), (b) (5), (b) (8)
(b) (2), (b) (5), (b) (8)	(b) (2), (b) (5), (b) (8)	(b) (2), (b) (5), (b) (8)
(b) (2), (b) (5), (b) (8)	(b) (2), (b) (5), (b) (8)	(b) (2), (b) (5), (b) (8)
(b) (2), (b) (5), (b) (8)	(b) (2), (b) (5), (b) (8)	(b) (2), (b) (5), (b) (8)
(b) (2), (b) (5), (b) (8)	(b) (2), (b) (5), (b) (8)	(b) (2), (b) (5), (b) (8)
(b) (2), (b) (5), (b) (8)	(b) (2), (b) (5), (b) (8)	(b) (2), (b) (5), (b) (8)

In addition to the seven enterprise-level risks, six "of concern" risks were identified: (b) (2), (b) (5), (b) (8)

The Chair of the ERM Council sent a memorandum in July 2023 to the ERM Council and agency staff assigned as risk coordinators. The memorandum stated that the NCUA assigns risk coordinators to coordinate the review of programs and activities that are currently in place to address the enterprise-level risks, provide the ERM Council with semiannual written updates about how the risks were managed by the NCUA within the risk appetite statement, and provide an annual presentation regarding the risks to the ERM Council. The

memorandum included expectations for the annual presentation and listed additional training for the risk coordinators.

Results In Detail

The objective of our audit was to determine if NCUA adequately established, maintained, and used risk profiles to address enterprise-level risks.

Our audit determined that the ERM Council did not consistently establish, maintain, and use risk profiles to address each of its enterprise-level risks.[6] The NCUA needed to improve the ERM Council's monitoring and assessing of enterprise-level risks because the risks had a varied level of monitoring and analysis. Additionally, the ERM Council needed to improve how it communicates its decisions regarding risks to agency officials who implement the decisions, as appropriate. Without the ERM Council's effective monitoring and assessment of enterprise-level risks or communication and implementation of its decisions, the NCUA may not have made informed decisions to enable proactive mitigation and monitoring strategies to meet the risk appetite.

The detailed results of our audit follow.

NCUA's ERM Council Should Improve Monitoring and Assessing Enterprise-Level Risks

We determined that the ERM Council did not regularly apply an approach consistent with the NCUA's ERM framework to assess and monitor all enterprise-level risks. The ERM Council did not regularly evaluate whether all enterprise-level risks were within the risk appetite or if the risk response strategies effectively mitigated risk. Without sufficient monitoring and regular assessment of enterprise-level risks at the organizational-wide level, there may be gaps in the ERM Council's awareness of the agency's response to risks and a potential lack of consensus regarding whether a risk was managed within risk appetite or if programmatic strategies effectively mitigated the risk. This may limit the agency's ability to make fully informed decisions, prioritize risks, and enhance resilience by enabling proactive mitigation and monitoring strategies to meet the risk appetite.

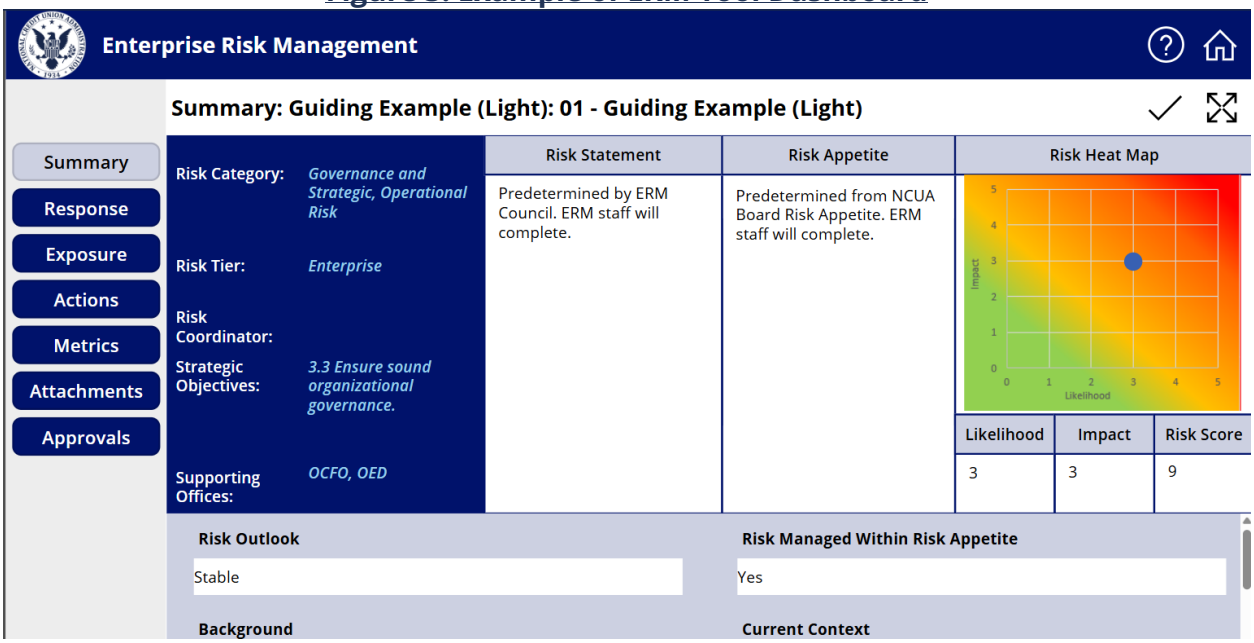
Details

The OCFO ERM staff developed an ERM tool to facilitate the ongoing risk monitoring and reporting of enterprise risks. The ERM tool is a customized dashboard used to capture risk response and monitoring activities for enterprise-level risks. The tool includes the components found in a risk profile. Using the tool, risk coordinators may document

[6] Findings related to the ERM Council are not indicative of agency monitoring or managing the risk at the office-level, which is outside the scope of the audit.

changes to an enterprise risk or agency's response to the risk, identify related emerging risks, collaborate with Council members or other senior-level staff with direct responsibility or oversight of risk-related activities, provide initial input, and respond to feedback from the ERM Council resulting from its review of the content in the ERM tool.

Figure 3: Example of ERM Tool Dashboard



We reviewed the ERM tool and documentation from ERM Council meetings, including meeting minutes, to determine if risk profiles had been completed or, if not, whether there was sufficient information available to convey all the elements of a risk profile. We found that risk profiles were not complete for every enterprise-level risks and enterprise-level risks were not regularly updated within the tool or briefed to the ERM Council to determine if risk response strategies effectively were mitigating risk and if risks were managed within the agency's risk appetite.

Three enterprise-level risks had complete profiles in the ERM tool as of August 2025. In addition, ERM Council minutes demonstrated the Council's extensive review of an additional risk, which was evidenced by multiple presentations and discussions, although the review was not formalized in a risk profile. The OIG noted that there were some inconsistencies or discrepancies in how certain elements were documented in the ERM tool between different risk profiles. Use of the ERM tool would address the necessary elements of a risk profile if used for all risks.

We reviewed the ERM Council's meeting minutes to evaluate evidence of its monitoring and updating of all enterprise-level risks. Although the ERM Council did not meet each quarter throughout the scope period as required by the charter, it met at least four times during 2023 (three times in the first quarter and once in the third quarter), significantly more frequently in 2024 (seven ERM Council meetings during the first three quarters and four

additional meetings to discuss one of the enterprise-level risks during the fourth quarter), and once during the first quarter of the 2025.[7] When reviewing the ERM Council's meeting minutes for each enterprise-level risk, we determined that although meetings occurred throughout the scope period, the meetings did not address the monitoring of every enterprise-level risks.

The ERM Council charter provided that the Council establish and maintain a risk profile for all enterprise-level risks. That is consistent with the OMB A-123 (2016) guidance on establishing risk profiles. The July 2023 memorandum regarding risk coordinator assignments provided that the risk coordinators are responsible for providing the ERM Council semiannual written updates about how the NCUA managed risk within the risk appetite approved by the Board in 2022. Additionally, the risk coordinators are responsible for an annual presentation to the ERM Council about their written updates. Although the 2023 memorandum did not correlate written updates with an update to the risk profile, an updated risk profile could provide a cause for a written update. Additionally, the information session in 2024 for the risk coordinators identified that the ERM tool should be updated with monitoring information at least once per year with summarized updates at quarterly ERM Council meetings. This is consistent with the OMB A-123 (2016) guidance on at least annual risk profile updates. The information session indicated that the purpose of the monitoring phase of the framework was to implement an approach that manages and reports on enterprise risks and risk response activities in a relevant and timely manner to agency leadership. The objectives are to identify changes to enterprise risks and determine whether risk response strategies effectively mitigate the risk, track trends, and understand if risk is being managed within the agency's risk appetite, and inform agency leadership about exposures, challenges, and trade-offs, including as they relate to resources. The ERM Council approved a schedule at the start of 2024 that would have resulted in updates to all enterprise-level risks during the year, consistent with its guidance. Due to competing and emergent work demands at the NCUA, however, the risk coordinators were unable to complete all of the updates in 2024 and the Council agreed to postpone updates about some of the lower impact risks until 2025.

We conducted interviews with OCFO staff responsible for the ERM program, ERM Council members, and risk coordinators regarding their responsibilities for the risk profiles. We found that ERM Council members and risk coordinators had inconsistent understandings of their roles and responsibilities, which resulted in ineffective approaches to coordination and communication of risk monitoring. Additionally, we noted that the ERM Council only received briefings on some, but not all, enterprise-level risks to determine how the agency addressed risk exposure, and that such briefings were not regularly updated. Three enterprise-level risks were not briefed during the scope period.[8] Although interviewees

[7] The scope period for the audit only included the first 3 months of 2025.

[8] In 2025, after the audit scope period, risk coordinators briefed two additional enterprise risks to the ERM Council. However, there were no completed risk profiles for these risks in the ERM tool.

consistently noted the value of the ERM Council, they also noted that ERM responsibilities were collateral duties for the members and risk coordinators, which resulted in their providing less attention to those tasks compared to the responsibilities of their primary positions. ERM Council documents included proposed schedules by OCFO's ERM staff for intended completion of risk profiles and briefings that were not adhered to and later updated. An updated risk monitoring schedule was established by OCFO on June 26, 2025, which included a timeline through Q4 2026 to address enterprise-level risks and "of concern" risks over the course of 2 years.

We noted that the ERM tool included an option for capturing metrics to track a risk or measure if the risk is being effectively managed. We asked ERM staff regarding NCUA's approach to risk tolerance, which is the acceptable level of variance in performance relative to the achievement of objectives. ERM staff stated that the risk tolerance is derived from the Board-approved risk appetite statement, and that rather than establishing discrete thresholds for enterprise-level risks, the agency is focused on whether operational performance of programs related to the risk support or impede its ability to achieve strategic goals or objectives, as outlined in the agency's strategic plan. This enterprise-level coordination contrasts with more discrete office-level risks, where specific tolerance thresholds exist for specific processes or more routine deliverables. As needed, the NCUA's ERM program may consider office-level risk tolerance information when reviewing the agency's response to enterprise risks. The ERM staff noted that establishing and maintaining reporting processes for additional risk tolerance indicators would provide limited utility for an agency of the NCUA's size, while creating a redundant workload for the agency's staff.

Given that discrete enterprise-level risk tolerance thresholds are not a required component of a risk profile,[9] that NCUA enterprise-level risks are tied to specific strategic objectives, the reliance on office-level risk tolerance thresholds, and that the use of the ERM tool and maturity of the risk profiles may require the use of metrics eventually, the OIG determined that completion and regular updates of the risk profiles would provide more context to determine the necessity of implementing enterprise-level risk tolerances and that the agency's response is appropriate for the current maturity.

Recommendations

We recommend NCUA management:

1. Implement a regular assessment and briefing of all enterprise-level risks, such as through discussion of risk profiles at ERM Council meetings, on a frequency

[9] Risk tolerances should be considered to create a comprehensive enterprise-level risk profile. However, risk tolerances can be established at the program, objective or component level.

commensurate with risk exposure to monitor that each risk is managed within risk appetite.

Management Response

Management agreed with our recommendation and will implement it by March 31, 2027.

OIG Response

We concur with management's planned action.

NCUA Needs to Improve Communication and Implementation of ERM Council Results

We determined that the ERM Council did not finalize processes that addressed responsibilities to communicate results after meetings or implement actions. The ERM Council was composed of various executives who did not represent all offices of the agency, and members took different approaches to how information was communicated and used. Stakeholders present at meetings did not explain to us how results of the meetings would be consistently communicated or used. Although ERM support staff noted that 2023 and 2024 year-end reporting to the NCUA Board documented the results of the ERM Council's work for those years, it is not clear whether agency officials and program managers consistently made informed decisions to enable proactive mitigation and monitoring strategies to meet the risk appetite.

Details

OMB Circular A-123 (2016) stated: "ERM seeks to open channels of communication so that managers have access to the information they need to make sound decisions."

COSO states: "Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization."

OMB's Playbook: ERM for the U.S. Federal Government (ERM Playbook)[10] states:

[10] The Chief Financial Officers Council (CFOC) and the Performance Improvement Council (PIC) released an update to the ERM Playbook as an inter-Council effort convened by the Office of Shared Solutions and Performance Improvement of the General Services Administration. The updated Playbook resulted from the efforts of a working group of ERM practitioners who are members of the ERM community of practice from over 50 federal agencies and included cross-functional representation.

> As an agency develops its risk governance structure, it is important it promotes communication and consultation with stakeholders. This will result in the identification of risks and response strategies that include the perspectives of program managers and key stakeholders. The governance structure needs to be built on the understanding that stakeholders can be internal or external to the agency. Agencies should consider the desired outputs of communication and consultation and decide where in the risk process to engage stakeholders. Communications can include formal and informal meetings with internal and external stakeholders, verbal or written reports, surveys, or emails, and meetings with teams to address specific risks, programs, objectives, or leadership activities. Part of the ERM process will be to define and establish documentation requirements and reporting methods.

The revised OMB A-123 states: "Information should travel in all directions (across, and up and down within an organization) to ensure that all appropriate members of the organization are informed and that decisions and actions of different units are communicated and coordinated."

As identified in the prior section, the ERM Council met multiple times during the audit scope period to discuss enterprise-level risks. Meeting minutes were documented and included in an annual summary to the Board.

We reviewed a draft ERM fundamentals document that established early expectations of the ERM program. Although this document was never finalized, it identified roles and responsibilities for senior leadership, a communication strategy, and provided that the ERM program would:

- facilitate transparency of enterprise risks to internal and external stakeholders,
- would include monitoring results and analysis are reported to senior leaders and used to assess significant risks,
- provide access to information that would enable risk-based decision making,
- allow senior leaders and managers to access risk information real-time, and
- support execution of risk response plans at the leadership level.

We conducted interviews with ERM staff, ERM Council members, and risk coordinators to learn how risk profiles or related risk information were communicated and used. ERM Council membership represented many of NCUA's offices but not all executive-level offices. Some of the interviewees recently joined the ERM Council due to staff departures from the Voluntary Separation Program (VSP) and had limited time in the role. The interviews demonstrated that there were no consistent approaches or clear expectations for how risks should be communicated outside the ERM Council or implementation of ERM Council decisions. Rather, sharing or using risk information varied in degree among Council members.

Recommendation

We recommend NCUA management:

2. Clarify how the ERM Council should communicate risk results to agency officials who implement decisions.

Management Response

Management agreed with our recommendation and will complete this by March 31, 2027.

OIG Response

We concur with management's planned action.

Appendix A

Objective, Scope, And Methodology

We developed our objective for this engagement based on OIG's 2025 Annual Work Plan. Specifically, our objective was to determine if the NCUA has adequately established, maintained, and used risk profiles to address enterprise-level risks.

To accomplish our audit, we performed fieldwork related to the NCUA's ERM risk profiles and applicable procedures, documentation, and controls. The scope covered ERM risk profile activities between January 1, 2023, to April 1, 2025.

To achieve our objective, we performed the following:

- Interviewed personnel involved with identifying and monitoring enterprise-level risks and developing, maintaining, and using risk profiles;
- Reviewed available policies and procedures related to the identification and monitoring of enterprise-level risks and the development, maintenance, and use of risk profiles;
- Assessed risk profiles for adequacy and completeness as governed by OMB Circular A-123;
- Reviewed risk profiles, ERM Council meeting minutes, and related material to identify how information was communicated and used; and
- Evaluated related internal controls.

We did not significantly rely on computer-processed data to answer the audit objective. Although we relied on data generated from an NCUA system tool, the tool did not process any data and we relied on our analysis of information from interviews and supporting documents to evaluate the data and support our conclusions.

We conducted this audit between May 2025 through March 2026 in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. 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. Specifically, we assessed 5 of the 5 internal control components, and 11 of the 17 associated underlying principles defined in the Government Accountability Office's (GAO) Standards for Internal Control in the Federal Government. We determined that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We summarize in Table 2 below the internal control components and underlying principles we assessed.

Table 2: Internal Control Components and Underlying Principles Assessed

Component #1: Control Environment
Principle #2 – Exercise Oversight Responsibility
Principle #3 – Establish Structure, Responsibility, and Authority
Component #2: Risk Assessment
Principle #6 – Define Objectives and Risk Tolerances
Principle #7 – Identify, Analyze, and Respond to Risks
Principle #9 – Identify, Analyze, and Respond to Change
Component #3: Control Activities
Principle #10 – Design Control Activities
Principle #12 – Implement Control Activities
Component #4: Information and Communication
Principle #13 – Use Quality Information
Principle #14 – Communication Internally
Component #5: Monitoring
Principle #16 – Perform Monitoring Activities
Principle #17 – Evaluate Issues and Remediate Deficiencies

The report presents within the findings the internal control deficiency we identified. However, because our audit was focused on these significant internal control components and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

Appendix B

NCUA Management Response

NCUA

Memorandum

SENT BY EMAIL

DATE: May 18, 2026

TO: Inspector General Marta Erceg
Office of the Inspector General

FROM: Executive Director Larry Fazio
Office of the Executive Director

LARRY FAZIO
Digitally signed by LARRY FAZIO
Date: 2026.05.18 13:27:41 -04'00'

SUBJECT: Management Response - Audit of the NCUA's Enterprise Risk Management Risk Profiles

Thank you for the opportunity to comment on the OIG's draft report entitled *Audit of the NCUA's Enterprise Risk Management Risk Profiles*. The report makes two recommendations. The following is our response to the recommendations in the draft report:

Recommendation 1. Implement a regular assessment and briefing of all enterprise-level risks, such as through discussion of risk profiles at ERM Council meetings, on a frequency commensurate with risk exposure to monitor that each risk is managed within risk appetite.

Management Response:
Management concurs with this recommendation and will implement this by March 31, 2027.

Recommendation 2. Clarify how the ERM Council should communicate risk results to agency officials who implement decisions.

Management Response:
Management concurs with this recommendation and will complete this by March 31, 2027.

If you have any questions regarding this response, please contact Shameka Sutton at 703-548-2485 or ssutton@ncua.gov .

Appendix C

Acronyms and Abbreviations

Acronym	Term
AICPA	American Institute of Certified Public Accountants
CFO	Chief Financial Officer
CIO	Chief Information Officer
COSO	Committee of Sponsoring Organizations of the Treadway Commission
E&I	Examination and Insurance
ERM	Enterprise Risk Management
ERM COUNCIL	Enterprise Risk Management Council
FEI	Financial Executives International
FMFIA	Federal Managers Financial Integrity Act
GAO	Government Accountability Office
GPRA	Government Performance and Results Act
IIA	Institute of Internal Auditors
IMA	Institute of Management Accountants
NCUA	National Credit Union Administration
OBI	Office of Business Innovation
OCFO	Office of Chief Financial Officer
OCSM	Office of Continuity and Security Management

Acronym	Term
OIG	Office of Inspector General
OMB	Office of Management and Budget
ONES	Offices of National Examinations and Supervision
SIF	Share Insurance Fund
VSP	Voluntary Separation Program

NCUA
National Credit Union Administration

Office of Inspector General

NCUA OIG
1775 Duke Street
Alexandria, VA 22314

The OIG's mission is to prevent, deter, and detect waste, fraud, abuse, and misconduct in NCUA programs and operations; and to promote economy, efficiency, and effectiveness at the agency.

To report allegations of waste, fraud, abuse, or misconduct regarding NCUA programs, employees, contractors, or contracts, please contact us via our OIG Hotline | NCUA or call 1-800-778-4806.

NCUA website | www.ncua.gov
Oversight.gov | www.oversight.gov