NCUA
National Credit Union Administration

OFFICE OF INSPECTOR GENERAL

AUDIT OF THE NCUA'S GOVERNANCE OF INFORMATION TECHNOLOGY INITIATIVES

Report #OIG-21-06

September 28, 2021

Office of Inspector General

SENT BY EMAIL

TO: Distribution List

FROM: Inspector General James W. Hagen

SUBJ: Audit of the NCUA's Governance of Information Technology Initiatives

DATE: September 28, 2021

The National Credit Union Administration (NCUA) Office of Inspector General (OIG) conducted this self-initiated audit to assess the NCUA's governance over information technology (IT) initiatives. The objective of our audit was to determine whether the NCUA has an effective process for identifying, controlling, prioritizing, and implementing IT initiatives across the agency. The scope of our audit covered the period of January 1, 2016, through December 31, 2019. In addition, we considered Office of the Chief Information Officer's (OCIO) concerns regarding the funding of IT projects that fall outside of Operations and Maintenance (O&M) support and below the threshold of Capital projects.

Results of our audit determined that overall, the NCUA has an effective process for identifying, controlling, prioritizing, and implementing IT initiatives across the agency. However, we also determined the agency could make some improvements in its IT Investment Management program related to its policies and procedures and transparency, as well as ensuring certain functions of the Information Technology Oversight Counsel (ITOC) are clearer.

We are making four recommendations to NCUA management that we believe will help the agency improve its IT Investment Management program. In addition, regarding the CIO's concerns related to funding IT projects, we learned the ITOC is looking into these concerns; therefore, we are not making a recommendation to address this area.

We appreciate the cooperation and courtesies NCUA management and staff provided to us during the audit. If you have any questions on the report and its recommendations, please contact me at 703-518-6351.

Distribution List:
Board Chairman Todd M. Harper
Board Vice Chairman Kyle S. Hauptman
Board Member Rodney E. Hood
Executive Director Larry Fazio
General Counsel Frank Kressman
Deputy Executive Director Rendell Jones
Chief of Staff Catherine D. Galicia

OEAC Acting Director Sam Schumach
Chief Financial Officer Eugene Schied
Chief Information Officer Rob Foster

Attachment

TABLE OF CONTENTS

Section _____ **Page**

EXECUTIVE SUMMARY 1

BACKGROUND 2

RESULTS IN DETAIL.....6

Need to Document IT Investment Management Policies and Procedures.....6

Authority, Responsibilities, and Functions Need to be Clearer.....11

Transparency Needed in the IT Investment Management Process.....17

Funding Ad Hoc IT Requests Concern.....20

APPENDICES:

A. Objective, Scope, and Methodology 21

B. NCUA Management Response 22

C. Acronyms and Abbreviations.....24

EXECUTIVE SUMMARY

The National Credit Union Administration (NCUA) Office of Inspector General (OIG) conducted this self-initiated audit to assess the NCUA's governance over information technology (IT) initiatives. The objective of our audit was to determine whether the NCUA has an effective process for identifying, controlling, prioritizing, and implementing IT initiatives across the agency. The scope of our audit covered the period of January 1, 2016, through December 31, 2019.[1]

Our audit determined that overall, the NCUA has an effective process for identifying, controlling, prioritizing, and implementing IT initiatives across the agency. However, we also determined the agency could make some improvements in its IT Investment Management program. Specifically, we determined the NCUA:

- Needs to document its IT Investment Management policies and procedures;
- Needs to make the scope of the Information Technology Prioritization Council's (ITPC) authority, responsibilities, and functions clearer; and
- Needs more transparency in the IT Investment Management process.

We are making four recommendations in our report to correct the issues we identified. In addition, we considered the Office of the Chief Information Officer (OCIO) concerns expressed during the audit regarding the funding of IT projects that fall outside of Operations and Maintenance (O&M) support and below the threshold of Capital projects. However, the OCIO did not provide sufficient evidence to substantiate this concern, and we also learned the ITPC is already looking into this issue. Therefore, we did not make a recommendation regarding this concern.

We appreciate the cooperation and courtesies NCUA management and staff provided to us during this audit.

[1] We extended the scope of the audit to December 31, 2020 to obtain information only pertaining to emergent IT requests that occurred during 2020.

BACKGROUND

The NCUA is an independent federal agency that regulates, charters, and supervises federally insured credit unions. The NCUA's organizational structure consists of a Central Office, the Asset Management and Assistance Center, and three regional offices.[2] OCIO is responsible for ensuring the resilience of the NCUA's IT infrastructure, and the availability and reliability of its technological applications help ensure efficiency and effectiveness of the agency's workforce. OCIO's vision statement is to manage IT as a strategic resource to securely leverage the power of data.

IT Governance and IT Investment Management

IT governance consists of the leadership, structures, and processes that enable an organization to make decisions to ensure that its IT sustains and extends its strategies and objectives. It requires a clear understanding of the agency's strategic goals and objectives and a structure with repeatable processes to support decisions ensuring alignment of IT investments with those goals and objectives. IT governance ensures that IT decisions focus on:

- Evaluating and directing the use of IT to support the organization;
- Monitoring the use of IT to achieve plans;
- Using the IT strategy and policies to accomplish its purpose; and
- Aligning the IT strategy with the organization's goals.

Essentially, IT governance provides a structure for aligning IT strategy with business strategy.

IT Investment Management is a management process that provides for the pre-selection (identification), selection, control, and evaluation of business need-driven IT investments across the investment lifecycle. IT Investment Management:

- Uses structured processes to minimize risks, maximize return on investments, and support decisions to obtain, maintain, improve, migrate, or retire IT investments.
- Establishes a common language to: (a) organize IT investments and define their business value; (b) evaluate and prioritize the investments; and (c) effectively manage change.

[2] The three regional offices are the Eastern, Southern, and Western regions. However, for most of our audit's scope period (January 1, 2016 through December 31, 2019), the NCUA operated five regional offices, regions 1 through 5. The agency closed two of those offices at the end of 2018, and the current three-region structure became effective on January 7, 2019.

Benefits of a Structured IT Investment Management and IT Governance Program

The GAO has indicated IT projects can become risky, costly, unproductive mistakes, adding that federal IT projects too frequently incur cost overruns and schedule slippages while contributing little to mission-related outcomes. However, with proper management, investments in IT can improve organizational performance, with some organizations having realized substantial improvements in processing data and information.

By following a formal framework, organizations can produce measurable results toward achieving their strategies and goals. A formal program also takes stakeholders' interests into account, as well as the needs of staff and the processes they follow.

Federal Requirements and Guidance for IT Investment Management

The Clinger-Cohen Act of 1996[3] serves as the basis for the IT governance processes in use at federal agencies today. The Federal Credit Union Act exempts the NCUA from the Clinger-Cohen Act[4] but the NCUA can use the Act as guidance for best practices. The Clinger-Cohen Act:

- Defined responsibilities for CIOs, including management of IT spending and improvements in agency performance through information resources.

- Requires executive agencies to establish clearly defined IT Capital Planning and Investment Control (CPIC) processes to focus more on the results achieved through IT investments while streamlining the IT acquisition process.

In March 2004, the GAO published an IT Investment Management guide (GAO ITIM Framework) built around the select/control/evaluate approach described in the Clinger-Cohen Act.[5] Reflecting current accepted or best-practices in IT Investment Management, the GAO ITIM Framework is a maturity model composed of five progressive stages of maturity that an agency can achieve in its investment management capabilities.[6] The maturity stages include and describe a set of critical processes that must be in place for the agency to achieve each stage. The GAO indicates the select/control/evaluate model provides a systematic method for agencies to minimize risks while maximizing the returns of investments. The following describe the components of this model:

- Select phase – Includes screening, ranking, and choosing projects that will best support an agency's mission needs.

[3] Pub. L. 104-106, 110 Stat. 186 (February 10, 1996).
[4] Under the Federal Credit Union Act, most federal acquisition laws, including the Clinger-Cohen Act, do not apply to the NCUA. See 12 U.S.C. §§ 1766(i)(2), 1789.
[5] GAO Executive Guide: *Information Technology Investment Management, A Framework for Assessing and Improving Process Maturity* (March 2004 Version 1.1, GAO-04-394G)
[6] We used the GAO ITIM Framework's current accepted or best practices as a guide to help identify areas where the NCUA could improve its IT Investment Management program. The NCUA is not required to follow the GAO ITIM Framework.

- Control phase – Includes monitoring progress and taking corrective actions to ensure that as projects develop and expenditures continue, the project continues to meet mission needs at the expected levels of cost and risk.

- Evaluate phase - Comparing actual versus expected results after project implementation to: (a) assess the project's impact on mission performance; (b) identify any changes or modifications to the project that may be needed; and (c) revise the investment management process based on lessons learned.

The NCUA's IT Investment Management and Governance Structure and Budget

The NCUA established an agency-wide IT investment board, the Information Technology Prioritization Council (ITPC), in February 2013 to "review and prioritize new and emerging information technology initiatives and better align those IT investments with the NCUA's mission." Its current charter, dated April 2019, states that the ITPC is the NCUA's official governing body for prioritizing and recommending IT Capital Projects and that the ITPC's primary responsibility is to review and recommend selected IT Capital Projects for investment. The purpose of the ITPC is to set the strategic direction for information technology by prioritizing projects and better aligning IT investments with NCUA's mission and strategic plan.

The Deputy Executive Director and the CIO co-chair the ITPC with the following senior executive leadership comprising the remaining ITPC membership:

- Chief Financial Officer

- Director of the Office of Examinations and Insurance

- Director of the Office of Business Innovation

- Two Regional Office directors on a rotational basis

- Two Central Office directors on a rotational basis

As shown in Table 1 below, from 2016 through 2019, NCUA's budget for ITPC-recommended projects was $49.2 million, accounting for 78 percent of the agency's total $63.3 million capital budget:

Table 1.

NCUA Capital Budget / ITPC Project Budget - 2016 thru 2019			
Budget Year	**Capital Budget**	**ITPC Projects**	
		Budget	**% of Capital Budget**
2016[7]	$10.1M	$6.4M	63%
2017[8]	$15.8M	$11.8M	75%
2018[9]	$15.4M	$13.9M	90%
2019[10]	$22.0M	$17.1M	78%
Total	**$63.3M**	**$49.2M**	**78%**

[7] Source: Approved Board Action Memorandum, November 18, 2015.
[8] Source: NCUA 2017 – 2018 Budget Justification.
[9] Source: NCUA 2018 – 2019 Budget Justification.
[10] Source: NCUA 2019 – 2020 Budget Justification.

RESULTS IN DETAIL

The objective of our audit was to determine whether the NCUA has an effective process for identifying, controlling, prioritizing, and implementing information technology initiatives across the agency.

We determined that overall, the NCUA has an effective process for identifying, controlling, prioritizing, and implementing IT initiatives across the agency. However, we also determined the agency could make some improvements in its IT Investment Management program. Specifically, we determined the NCUA:

- Needs to document its IT Investment Management policies and procedures;
- Could make the scope of the ITPC's authority, responsibilities, and its functions clearer; and
- Needs more transparency in the IT Investment Management process.

The detailed results of our audit follow.

The NCUA Needs to Document its IT Investment Management Policies and Procedures

We determined the NCUA does not have documented Information Technology Investment Management policies and procedures. Although the NCUA attempted to implement an Information Resource Management (IRM) policy in 2018, we were informed it was not finalized due to negative feedback. We also determined the ITPC has not addressed the CPIC function of evaluating its IT projects (i.e., conducting post-implementation reviews (PIRs)). An NCUA official told us they believed the ITPC had not addressed this function because the agency was just in the beginning stages of having a centralized IT Investment Management review function. As previously mentioned, *GAO's Executive Guide: Information Technology Investment, A Framework for Assessing and Improving Process Maturity* (March 2004, Version 1.1) (GAO ITIM Framework) provides a benchmark of current accepted or best IT Investment Management practices. These IT Investment Management practices include an organization's need for documented policies and procedures. In addition, the GAO ITIM Framework indicates the select/control/evaluate model described in the Clinger-Cohen Act, provides a systematic method for agencies to minimize risks while maximizing the returns of investments. We believe that documenting IT Investment Management policies and procedures will help agency executives ensure consistent IT Investment Management practices and procedures and help facilitate advancing the maturity of the NCUA's IT Investment Management processes and capabilities.

Details

Documenting IT Investment Management Policies and Procedures

We determined that although the NCUA began formalizing its IT Investment Management structure and capabilities in 2013, it has not documented the policies and procedures to guide the ITPC, the ITPC's members, and the offices of primary interests (OPIs) in selecting, controlling, and evaluating the agency's IT investments and to guide the NCUA's IT governance processes.

The GAO ITIM Framework identifies "critical processes" (i.e., requirements) an organization must have in place to mature its investment management capabilities progressively from unstructured/ad hoc (Stage 1) to the most advanced stage at which organizations benchmark their processes against other "best-in-class" organizations (Stage 5). These critical processes (or requirements) include a set of "key practices" (i.e., organizational commitments, prerequisites, and activities) that, when fulfilled, implement the critical processes needed to attain a given maturity stage. Organizations must perform these key practices to effectively implement and institutionalize each critical process. The GAO ITIM Framework further guides that while an organization may have in place certain requirements at higher stages, the organization cannot attain a higher stage of maturity until it has institutionalized all the requirements for a particular stage and the requirements of the lower stages.

We determined there are 21 key practices throughout stages 2 through 5 that are categorized as organizational commitments. Fifteen of these 21 organizational commitments indicate the need for documented policies and procedures as follows:

- Stage 2 - Seven of the nine organizational commitments pertain to the need for documented policies and procedures, including:
    - A documented process directing the investment board's operations.
    - Selecting new IT proposals and ongoing projects.
    - Identifying and collecting information about IT projects and systems to support the investment management process.
- Stage 3 - Four of the five organizational commitments pertain to the need for documented policies and procedures, including:
    - Analyzing, selecting, and maintaining the investment portfolio.
    - Conducting post-implementation reviews.
- Stage 4 - Two of the three organizational commitments pertain to the need for documented policies and procedures such as evaluating and improving the performance of the IT portfolio.

- Stage 5 - Two of the four organizational commitments pertain to the need for documented policies and procedures such as improving the IT Investment Management process using benchmarking.

We also benchmarked against six executive branch agencies, including three regulatory agencies (which included another financial regulator), to determine whether they had documented IT Investment Management policies and procedures. We identified two or more documented IT Investment Management policies and procedures for five of the agencies and one documented policy for the other agency. These documents addressed IT Investment Management policies and procedures ranging from defining the roles, responsibilities, and requirements for agency IT capital planning to describing the IT governance framework or process. The following is a summary of some of the areas the agencies' IT Investment Management policies and procedures addressed:

Table 2.

Coverage of Benchmarked Agencies' IT Investment Management Policies and Procedures						
Area	**Agency**					
	1	**2**	**3**	**4**	**5**	**6**
IT Governance[11]	✓	✓	NA	✓	✓	✓
ITIM (CPIC) Process Requirements	✓	✓	✓	✓	✓	✓
ITIM (CPIC) Functions/Phases	✓	✓	✓	✓	✓	✓
ITIM (CPIC) Roles and Responsibilities	✓	✓	✓	✓	✓	✓
IT Investment-Related Definitions (e.g., major versus non-major IT investments)	✓	✓	✓	✓	✓	✓

An NCUA executive informed us that in March 2018, OCIO attempted to formally implement an IRM policy by issuing a 17-page final draft of an IRM Program policy to the OPIs for comment. The executive added that the Office of the Executive Director (OED) never signed or released the policy. Another NCUA official we spoke with believed the draft policy, which was intended

[11] IT governance consists of the leadership, structures, and processes that enable an organization to make decisions to ensure that its IT sustains and extends its strategies and objectives.

to address the Federal Information Technology Acquisition Reform Act[12] (FITARA), was too ambitious and not achievable, adding that it was rejected based on comments received. The NCUA executive also informed us that in October 2018, a 10-page IRM Program policy was sent to the OED for approval. The purpose of this final draft IRM Program policy was "[t]o establish the NCUA's Information Resource Management (IRM) Program, including specific requirements, a framework, and roles and responsibilities for effectively and efficiently planning and managing the agency's Information Technology (IT) resources." The official informed us the policy was not signed.

Evaluating IT Projects

We determined that although the ITPC is clearly responsible for selecting and controlling the NCUA's IT investments, it has not addressed the CPIC function of evaluating its IT projects (i.e., conducting PIRs). Specifically, we reviewed presentations from 21 meetings the ITPC held between January 2016 and December 2019 and determined the ITPC addressed what we assessed as CPIC select and control function activities and IT governance matters. However, we did not find any indication that the ITPC addressed the CPIC evaluate function under which PIR activities align even though an NCUA official informed us the agency implemented the new HR Links system[13] in June 2018 within the scope period of our audit.

We benchmarked against the other agencies to determine whether they followed the CPIC select/control/evaluate model as included as a best practice in the GAO ITIM Framework. We determined all six agencies followed the select/control/evaluate CPIC approach.[14]

We asked a senior executive (and ITPC member) about the lack of discussions or activity pertaining to PIRs (i.e., the CPIC evaluate function). The official surmised that the original ITPC responsibilities did not address that function because at the time, the NCUA was just beginning to have a centralized review function for its IT investments. The official added that as the NCUA has continued to increase the agency's maturity in reviewing IT investments, officials have tried to have a more robust governance process. Regarding the agency's efforts to address post-implementation reviews, we learned management was in the process of drafting an update to its ITPC charter that would give the ITPC the added responsibility to "[r]equest that Post Implementation Reviews (PIR) …be conducted…."

During this audit, we advised NCUA management in a February 2021 Notice of Findings and Recommendations (NFR) that although we believed this was a positive step towards the agency

[12] Pub. L. No. 113-291, 128 Stat. 3292, 3438-50 (December 19, 2014). FITARA established specific requirements related to Federal IT acquisition, including consolidating authority for agency CIOs, reviews of agency IT investment portfolios, enhanced transparency, and improved risk management in IT investments. FITARA applies to CFO Act agencies, which the NCUA is not, but OMB M-15-14 (June 10, 2015), Management and Oversight of Federal Information Technology, which implemented FITARA, provided that all Executive Branch agencies are encouraged to apply the principles described in this guidance to their management of IT, consistent with their legal authorities.
[13] The official clarified that the "Human Resources System" project was implemented as HR Links.
[14] As indicated in GAO ITIM Framework, the Clinger-Cohen Act of 1996 describes the select/control/evaluate approach.

conducting PIRs going forward, it was not clear *how* the agency would implement its PIR activities.

We believe that by documenting its policies and procedures, NCUA executives will institutionalize the agency's IT Investment Management practices and help ensure consistent IT Investment Management procedures necessary for the inevitable succession of executives, management, and staff. In addition, documented policies and procedures will help advance the maturity of the agency's IT Investment Management processes and capabilities.

In April 2021, after the we issued the NFR, NCUA officials gave the OIG the opportunity to provide feedback on a five-page draft charter they were updating. The updated draft charter expands upon the IT Oversight Council's (ITOC) responsibility to conduct PIRs.[15] Specifically, the updated draft charter includes why PIRs are to be conducted and the activities associated with conducting a PIR. We believe this provides the additional guidance that was missing in the prior version of the draft charter. However, we also suggested to management they address: (1) what is meant in the charter by conducting PIRs "where appropriate"; and (2) the criteria the ITOC would use to select the projects that would undergo a PIR. We believe the agency should include this level of detail in its IT Investment Management policies and procedures.

To institutionalize, ensure consistency in, and facilitate the NCUA in maturing its IT Investment Management processes, we are making one recommendation.

Recommendations

We recommend NCUA management:

1. Document and publish Information Technology Investment Management policies and procedures to include definitions, roles, responsibilities, and processes associated with information technology governance and selecting, controlling, and evaluating information technology investments.

Management Response

Management agreed with our recommendation. Management indicated they plan to review the previous iterations of the IT Investment Management policies and re-draft them to better define roles, responsibilities, and processes associated with IT governance and selecting, controlling, and evaluating IT investments. Management estimated a completion date of March 2022.

OIG Response

We concur with management's planned actions.

[15] The updated draft charter changes the name of the ITPC to the IT Oversight Council (ITOC).

The NCUA Needs to Make its Authority, Responsibilities, and Functions Clearer

We determined the NCUA could make the scope of the ITPC's authority, responsibilities, and its functions clearer. The GAO ITIM Framework identifies *instituting an investment board* as a critical process that we believe will guide the NCUA in making the ITPC's authority, responsibilities, and functions clearer. Specifically, the GAO ITIM Framework addresses this process of defining "the membership, guiding policies, operations, roles, responsibilities, and authorities for each designated board and, if appropriate, each board's support staff…." An NCUA senior official told us they believed that the ITPC's original charter was just in the beginning stages of having a centralized IT Investment Management function and that the agency has been trying to increase its maturity and have a more robust governance process. We believe this contributed to why the current charter is not more comprehensive and clearer. The NCUA updated its charter once between December 2015 and April 2019 and has been in the process of drafting additional updates; however, the agency has not finalized an updated charter to date. We believe that developing a more comprehensive ITPC charter will make the ITPC's authority, responsibilities, and functions clearer.

Details

We reviewed the NCUA's current April 2019 one-page ITPC charter and the activities the ITPC conducted during its meetings. We determined that although it is clear the ITPC has authority over and responsibility for the NCUA's IT Investment Management program, the charter could more clearly address:

- The scope of the ITPC's investment management authority,
- The scope of the ITPC's responsibilities and functions, and
- The responsibilities of the ITPC members.

<u>Scope of the ITPC's IT Investment Authority</u>

The ITPC charter stipulates the ITPC is "the official governing body for prioritizing and recommending ***IT Capital Projects*** [emphasis added] …" with "[t]he primary responsibility…to review and recommend ***selected IT Capital Projects*** [emphasis added] for investment." However, it is not clear what the parameters are for the "selected IT Capital Projects" that fall within the scope of the ITPC's IT Investment Management authority, such as:

- Project type(s) (e.g., all IT Capital investments, IT hardware acquisitions, commercial-off-the-shelf acquisitions, software development projects, etc.).
- Project threshold(s) (e.g., estimated labor hours, initial capital costs, multi-year/ life-cycle capital costs, etc.).

We asked ten current and prior ITPC members the definition of an IT Capital Project as it pertains to the ITPC's authority. The executives' responses included that it has not been defined,

that it is an accounting question, or generally that it is a large IT project. One executive, who helped create the ITPC, said that what constitutes an IT Capital Project is something the ITPC has struggled with. Another of the executives explained that he views it from an accounting perspective, adding merely that it determines which budget funds the project. We learned that for the purposes of NCUA Budget Execution[16] a "capital budget," as it pertains to IT, includes "any investment project over $100,000 related to…infrastructure, software and hardware investments…." We believe this definition represents one example of how the NCUA could delineate the parameters of the selected IT Capital Projects over which the ITPC has authority.

Scope of the ITPC's Responsibilities and Functions

The current charter: (a) not only stipulates the ITPC is the official governing body for prioritizing and recommending IT Capital Projects; but also (b) states the ITPC sets the strategic direction for IT investment, adoption and use by prioritizing projects and aligning IT investments with the mission of the NCUA, fostering transparency and accountability in the management of agency IT resources.

Based on our review, it is clear the ITPC is the NCUA's IT investment board[17] and, as such, is responsible for defining and implementing the NCUA's IT investment management processes and functions. We also believe it is evident that the ITPC has a role in agency IT governance (e.g., strategic direction and governing).[18] However, we believe the agency could more clearly specify the scope of the ITPC's investment management responsibilities and functions and the scope of its IT governance responsibilities to help keep the ITPC focused on operating in accordance with its assigned responsibilities and functions.

Specific to IT Investment Management, it is not clear what the full scope of the ITPC's assigned responsibilities and functions are (or should be) in carrying out its primary responsibility to review and recommend projects for investment and whether the scope of the ITPC's responsibilities and functions includes or should include reviewing the status of ongoing projects and conducting PIRs. We reviewed the ITPC's minutes and presentations from the meetings it conducted between January 2016 and December 2019 and determined the ITPC:

- Spent 42 percent of its time (22 hours) on CPIC "select" functions, which fit within its primary responsibility to review and recommend IT investments.[19] However, the charter

[16] NCUA Instruction 2020.3 (Rev. 1), "Guidelines for Budget Execution" (May 20, 2016)
[17] A decision-making body made up of senior program, financial, and information managers that is responsible for making decisions about IT projects and systems based on comparisons and trade-offs among competing projects, with an emphasis on meeting mission goals.
[18] As indicated in OMB Memorandum M-09-02, Information Technology Management Structure and Governance Framework (October 21, 2008), this responsibility could include setting agency-wide IT policy, including all areas of IT governance such as enterprise architecture and standards, IT capital planning and investment management, IT asset management, IT budgeting and acquisition, IT performance management, risk management, IT workforce management, IT security and operations, and information security. The NCUA is not required to follow OMB guidance.
[19] The GAO ITIM Framework indicates that during the select phase the organization: (1) identifies and analyzes each project's risks and returns before committing significant funds to any project and (2) selects those IT projects that will best support its mission needs.

does not identify the ITPC's specific responsibilities and functions such as identifying (and periodically reviewing) the criteria the ITPC uses for prioritizing and selecting IT investments to recommend to the NCUA Board.

- Spent 28 percent of its time (15 hours) on CPIC "control" functions. However, the charter does not identify control functions as part of the ITPC's responsibilities such as formally assigning the ITPC the responsibility to periodically assess and report the status of ongoing IT projects and associated timeframes or indicating whether the ITPC is responsible for making decisions whether to continue, adjust, or end those projects.[20]

However, as previously mentioned, we did not find any indications that the ITPC discussed or conducted CPIC evaluate activities associated with PIRs even though we are aware the NCUA implemented at least one ITPC project within the scope period of our audit.[21] The charter does not identify the CPIC evaluate function as an ITPC responsibility, such as when and how often to conduct PIRs of the projects that fall within the scope of its authority.

Specific to "IT governance," we determined the ITPC spent 30 percent of its time (16 hours) addressing IT investment strategy issues, which we believe fit within its chartered *purpose* to set the strategic direction for IT investment, adoption, and use. However, the charter does not specify the ITPC's roles and responsibilities as they pertain to agency IT strategy, such as its role in establishing the NCUA's Enterprise Business IT Vision and Strategy.

We also benchmarked against five IT investment review-related board charters from three other federal agencies and determined that the charters, ranging from four to seven pages, were much more detailed and specific than the ITPC's one-page charter, providing a clearer understanding of those boards' authorities, responsibilities, and functions. For example:

- One of the charters detailed 19 functions of the IT investment board (e.g., approve all IT investments, approve the IT business architecture and roadmap, etc.).

- One agency had three IT investment board charters, which:

    - Detailed the IT investment board's governance responsibilities and functions (e.g., recommend the priority order of programs, projects or other investments; approve, defer or reject a proposed investment; conduct periodic reviews of the IT portfolio, programs, projects or other investments, etc.).

    - Incorporated the IT investment board's activities that support the CPIC select, control and evaluate phases (e.g., the boards' responsibilities during the proposal review process (select phase); to ensure projects meet cost, schedule and

[20] The GAO ITIM Framework indicates that during the control phase the organization ensures that, as projects develop and investment expenditures continue, the project continues to meet mission needs at the expected levels of cost and risk.
[21] An NCUA official informed us the NCUA implemented HR Links in June 2018.

performance goals (control phase); and to periodically review the results of completed programs, projects or other investments (evaluate phase)).

ITPC Member Responsibilities

Regarding the responsibilities of its members, the NCUA's ITPC charter indicates only that:

- The Chair and Co-Chair are to "…*set the agenda and prepare materials for Council meetings*…."
- Members are "…*required to attend*..." the meetings and are "…*entitled to one vote*…."

In contrast, the other agencies' charters provided much more detail on the responsibilities of the boards' members and in some cases the boards' support staff. For example:

- One of the charters detailed:
  - The board chair's responsibilities (e.g., serve as the decision authority, report decisions, and communicate issues on behalf of the board, etc.)
  - The board members' responsibilities (e.g., review background/decisional materials, represent discussions, issues, and decisions from external entities, etc.)
  - The responsibilities of the board's IT governance lead member (e.g., record and distribute meeting minutes, monitor final decision outcomes, etc.)
- Another charter detailed the responsibilities of the board's IT investment staff (e.g., prepare and submit status reports on investment proposals, document board issues, actions, and decisions, etc.).

As previously discussed, the GAO ITIM Framework identifies "critical processes" an organization must have in place to mature its investment management capabilities.[22] One of the critical processes at Stage 2[23] is "Instituting the Investment Board," which is the process of defining "the membership, guiding policies, operations, roles, responsibilities, and authorities for each designated board and, if appropriate, each board's support staff…." This definition "provides the basis for each board's investment selection, control, and evaluation activities."

One of the prerequisites for this critical process is "[e]ach board's span of authority and responsibility is defined…" with "criteria [that] can be based on cost, benefit, schedule and risk thresholds, the number of users affected…the life cycle phase of an IT investment…, or other comparable or useful measures."

[22] Examples of critical processes at stages 2 through 5 are selecting an investment, evaluating the portfolio, managing the succession of information systems, and optimizing the investment process.
[23] Stage 2 of maturity is where the organization "builds the foundation for current and future IT investment success…."

We also reviewed the five charters to determine whether they addressed similar content (e.g., the scope of the boards' responsibilities and functions, membership, etc.) We determined the five charters addressed similar content in the following areas:

Table 3.

Other Agencies' Benchmarked Charters: Areas of Common Coverage					
Area	**Charter**				
	1	**2**	**3**	**4**	**5**
Purpose of Charter	✓	✓	✓	✓	✓
Purpose/Mission of Group	✓	✓	✓	✓	✓
Authority (governing policies, regulations)	✓	✓	✓	✓	✓
Group Functions	✓	✓	✓	✓	✓
Membership/Structure	✓	✓	✓	✓	✓
Membership Responsibilities	✓	✓	NA	NA	NA
[Support] Staff Responsibilities	✓	✓	NA	NA	NA
Meetings (e.g., frequency, attendance, quorum, governance)	✓	✓	✓	✓	✓
Minutes/Records	✓	✓	✓	✓	✓

In addition, we identified and reviewed tips or suggestions the NCUA could consider as potential best practices for the ITPC charter to assist the agency in building its IT Investment Management foundation. The guidance we reviewed includes that:

> "Activities, Duties, and Responsibilities…[are] the meat and bones of the committee's charter. It spells out exactly what the committee needs to do. More importantly, it outlines what the committee is responsible for."

Best practices also guide that:

> "Committee charters help [a] board to meet its legal and regulatory commitments and…. The wording in the charter orients…committee members to the committee's structure and its rules. The work that committees perform

> acts as an extension of [a] board's important work, providing a comprehensive and effective process for meeting board goals and objectives."

Although the ITPC published two versions of its charter between December 2015 and April 2019, one senior official/ITPC member we interviewed stated the charter needs to be updated.[24] Specifically, the official pointed out that the charter did not address how IT initiatives align with the NCUA's missions and goals, effective management of initiatives and providing regular status reports to management. The official added that the agency needs clearer roles, responsibilities, policy, and procedures. We learned later that NCUA officials were drafting a three-page update (draft charter) to its current April 2019 one-page charter (current charter). We believe this three-page draft charter was more comprehensive than its current one-page charter in addressing the scope of the ITPC's IT Investment Management authority and responsibilities. However, we also believe the draft charter could be clearer regarding which IT investments fall within the ITPC's authority. As previously mentioned, in April 2021, the NCUA provided the OIG with an opportunity to provide feedback on its more recently updated five-page draft charter (updated draft charter). We determined the updated draft charter makes it clear which IT investments fall within the ITOC's scope of authority. However, we also provided comments we believe could further improve the charter's clarity in other areas, including:

- Listing the governing laws, regulations, and policies that provide the ITOC's authority.
- If applicable, adding back the ITOC's responsibility for setting the strategic direction for the investment, adoption, and use of the NCUA's information technology (i.e., IT governance).
- Including the project screening criteria, the ITOC considers in determining which "IT investments…best meet the current needs of the NCUA."

To improve clarity in the ITPC's IT Investment Management authority, responsibilities, and functions, we are making one recommendation.

Recommendations

We recommend NCUA management:

2. Finalize and publish an updated Information Technology Oversight Council charter that more comprehensively addresses and delineates the Information Technology Oversight Council Information Technology Investment Management authority, responsibilities, and functions.

Management Response

Management agreed with our recommendation. Management indicated they will update and finalize the ITOC charter to reflect the input received from this audit. In addition, management

[24] The ITPC published its first charter in December 2015 and updated it in April 2019.

indicated they will publish the updated charter which will comprehensively address and delineate the ITOC's IT investment management authority, responsibilities, and functions. Management estimated a completion date of January 2022.

OIG Response

We concur with management's planned actions.

Transparency Needed in the IT Investment Management Process

We determined NCUA Board members do not receive clear and sufficient information regarding ITPC projects to assist them in making more informed IT Investment Management decisions. The NCUA's strategic values and the ITPC charter require transparent communications. In addition, in response to the OIG's 2018 Records Management Report (OIG-18-05, March 14, 2018), the NCUA included language in the current April 2019 ITPC charter to provide the Board with more detailed information regarding the agency's IT investments. However, we learned the NCUA had removed this requirement while drafting updates to the ITPC charter. In providing feedback to the NCUA regarding the draft ITPC charters, we requested that management include that requirement again. We believe that by providing Board members with more detailed information regarding the agency's IT investments, the NCUA will make its IT Investment Management process more transparent.

Details

We learned that although Board members receive a list of IT projects the ITPC submits for funding, the Board does not receive information regarding: (a) all the IT projects the OPIs submit to the ITPC for consideration; (b) the ITPC's rating and ranking of the submissions it uses to arrive at the list of IT projects it submits to the Board for budget approval; and (c) whether a project request is legally or statutorily mandated.

The NCUA Strategic Plan states "one of the NCUA's five values is transparency—to be open, direct and frequent in communications." Also, the ITPC's current April 2019 charter indicates the purpose of the ITPC includes fostering transparency and accountability in managing the NCUA's IT resources.

GAO's Green Book[25] states:

- Information and communication - analyze and discuss information relating to the entity's achievement of objectives.

- Reporting lines are defined at all levels of the organization and provide methods of communication that can flow down, across, up, and around the structure.

[25] GAO-14-704G Standards for Internal Control in the Federal Government states (September 2014).

- Effective information and communication are vital for an entity to achieve its objectives.
- Management should internally communicate the necessary quality information to achieve the entity's objectives.

During our audit, we learned that although NCUA management agreed to implement our recommendation from the Records Management Report to provide more information to the Board, they have failed to do so. Specifically, in 2018 the OIG recommended NCUA management implement a change to the protocol of all Board briefings that occur as part of the ITPC project evaluation to include a listing of all office projects and highlight those that are associated with a statutory or other legal requirement as well as the rating and ranking of each project.

In response to the OIG's recommendation, NCUA's Executive Director at that time stated: "We will provide all board offices with a project list containing the rating and ranking of each project and highlight any statutory or other legal requirement relevant to the projects following each ITPC ranking determination."

In October 2019, the OIG reviewed the status of this recommendation and learned from NCUA management that the ITPC would begin sharing a list of projects with Board members and had updated its ITPC charter on April 12, 2019, to state: "Board Reporting: The ITPC will provide the Board with a prioritized list of IT capital projects submitted by the OPIs, highlighting requests for statutory or other mandated requirements."

Based on what NCUA management had advised the OIG and the updated ITPC charter, the OIG closed the recommendation from report OIG-18-05 in October 2019.

As previously mentioned, we learned that NCUA management had not provided detailed information to the Board from Board members who informed us they are not receiving a listing of all office projects from the ITPC. For example, one Board member stated he does not receive OPI submissions the ITPC has not approved to forward for funding; he indicated he would like to receive such information. The Board member added that he receives ITPC decisions primarily during the budget review and approval process, but never at a granular level. He stated he would prefer to see more details especially on big projects with considerable costs. He also noted that Board members generally view agency operations from a different perspective, indicating that if he were to review the comprehensive list of all OPI submissions, he might see a proposed project worthy of further attention. The Board member further informed us that it would be helpful to know about projects the ITPC may have rejected (or deferred), because he is aware of projects on which peer agencies are working.

Another Board member told us that although the ITPC prioritizes projects and sends the list of its approved projects to the Board as part of the budget process, he does not see the details about the projects from the ITPC's meetings. The Board member added that the Executive Director and the

Chief Financial Officer develop the budget to present to the Board, and noted he only receives what is presented to him as the priorities.

As noted on the previous page of this audit report, we requested that management add back to the charter the requirement to provide a more comprehensive project listing to the Board. We believe that providing Board members with a comprehensive list of all OPI-proposed projects and the ITPC meeting minutes would make the IT Investment Management process more transparent. Further, it would help Board members to not only have a more comprehensive understanding of the agency's IT issues and investment efforts, but also enable them to better understand IT issues and efforts raised by peer agencies.

To improve transparency in the IT Investment Management process, we are making two recommendations.

Recommendations

We recommend NCUA management:

3. Keep the language from the April 2019 charter, or include similar language in its new charter, requiring the NCUA Information Technology Oversight Council to provide a rated and ranked listing of all office of primary interest-proposed projects to the NCUA Board, highlighting those that are statutorily or legally required.

Management Response

Management agreed with our recommendation. Management indicated they will keep the language from the current draft ITOC charter and will add a comprehensive list of all IT investments. In addition, management indicated the ITOC will detail the investments which are and are not recommended for funding in its funding request submissions to the NCUA Board. Management indicated it is set to begin this practice with the 2022-2023 budget process.

OIG Response

We concur with management's planned actions.

4. Include language in the Information Technology Oversight Council's charter requiring NCUA officials to provide the Information Technology Oversight Council meeting minutes to the NCUA Board.

Management Response

Management agreed with our recommendation. Management indicated they will update the ITOC charter to include the submission of ITOC minutes to the NCUA Board. Management estimated a completion date of January 2022.

OIG Response

We concur with management's planned action.

Funding Ad Hoc IT Requests Concern

During our entrance conference, the CIO expressed concerns that OCIO receives ad hoc priority IT requests that it must plan, develop, and sometimes complete without prior designated funding. The CIO indicated these special requests fall between its O&M support but below the [ITPC] Capital project threshold,[26] which the CIO has caused his office to shift its existing resources from its day-to-day IT operational support mission without an assurance of reimbursement. During our audit, another senior agency official suggested that a reserve fund[27] could fund ad hoc projects. We asked the OCIO for specific examples of ad hoc taskings that were not reimbursed and how they adversely impacted OCIO's support mission. The OCIO only provided one example, which occurred in 2018.[28] When we asked OCIO for additional examples, it provided us with several examples of ad-hoc COVID-related projects that it worked on in 2020. However, we learned the OCIO was reimbursed for these ad-hoc projects as part of the NCUA's mid-session reprogramming process. Consequently, we did not have sufficient evidence to substantiate the OCIO's concerns.

We learned the ITPC briefly discussed the challenges related to this issue during its February 2020 meeting in which the ITPC tasked the OCIO to provide it with an inventory of all its ad hoc work. We also noted on that meeting's agenda the ITPC included the importance of defining O&M and capital, which we determined is an issue.[29] In addition, we learned that the NCUA has a formal documented process for reprogramming budgets for unfunded requests/ad-hoc expenses.[30]

Because we were unable to obtain sufficient evidence to substantiate a potential issue and considering that: (1) the NCUA has an existing process to address unfunded requests, and (2) the ITPC is currently looking into this issue, we determined the best course of action would be to allow NCUA management to work out internally any issues that may exist. Therefore, we are not making any recommendations at this time.

[26] On page 11 and page 12 of this report, we discussed the NCUA's lack of clarity surrounding the threshold of IT Capital projects.
[27] A reserve fund is a contingency set aside to address unanticipated funding requirements that emerge during the year for a budget.
[28] The 2018 request was for OCIO to develop a dividend calculator, which was unanticipated but considered a high priority project requested by the NCUA Board.
[29] On page 11 and page 12 of this report, we discussed the lack of clarity surrounding the threshold of IT Capital projects.
[30] NCUA Instruction 2020.3 (Rev.1), *Guidelines for Budget Execution,* May 20, 2016.

Appendix A

OBJECTIVE, SCOPE, AND METHODOLOGY

We developed our objective for this engagement based on the OIG's 2020 Annual Performance Plan. Specifically, our objective was to determine whether the NCUA has an effective process for identifying, controlling, prioritizing, and implementing IT initiatives across the agency.

To accomplish our audit, we performed fieldwork relating to OCIO and OCFO as well as ITPC activities in the NCUA's Central Office in Alexandria, VA. The scope of this audit focused on IT investment-related activities and initiatives from January 1, 2016 to December 31, 2019. However, we extended the scope to December 31, 2020 to obtain information pertaining only to emergent IT requests that occurred during 2020. To achieve our objectives, we:

- Reviewed draft and final ITPC charters;
- Reviewed Board Action Memorandums, Budget Justifications, and budget policies and procedures;
- Reviewed ITPC meeting minutes and associated presentations;
- Interviewed various NCUA management and staff, including current and past members of the ITPC;
- Interviewed the NCUA Board Chairman and Board members, and
- Benchmarked against selected federal agencies' IT Investment Management program policies, procedures, and charters.

We performed fieldwork from January 2020 through August 2021. We conducted this audit 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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix B

NCUA MANAGEMENT RESPONSE

National Credit Union Administration
Office of the Executive Director

SENT BY EMAIL

TO: Inspector General, James Hagen

FROM: Executive Director, Larry Fazio LARRY FAZIO Digitally signed by LARRY FAZIO Date: 2021.09.24 16:59:10 -04'00'

SUBJ: Audit of the NCUA's Governance of Information Technology Initiatives

DATE: September 24, 2021

Thank you for the opportunity to review the draft Report on *The NCUA's Governance of Information Technology Initiatives*. We are pleased the audit determined that the agency overall has an effective process for identifying, controlling, prioritizing, and implementing information technology initiatives.

In addition, the report provided good recommendations for some improvements in the NCUA's Information Technology Investment Management program. We agree with your assessment and have begun to take steps to address the report's four (4) recommendations. Our specific responses to the recommendations are as follows:

OIG Recommendation 1: Document and publish Information Technology Investment Management policies and procedures to include definitions, roles, responsibilities, and processes associated with information technology governance and selecting, controlling, and evaluating information technology investments.

Management Response: Management concurs. We will review the previous iterations of Information Technology Investment Management policies and re-draft them to better define, roles, responsibilities, and processes associated with information technology governance and selecting, controlling, and evaluating information technology investments. The estimated completion date is March 2022.

OIG Recommendation 2: Finalize and publish an updated ITOC charter that more comprehensively addresses and delineates the ITOC's IT investment management authority, responsibilities, and functions.

Management Response: Management concurs. We will update and finalize the ITOC charter to reflect the input received from this audit. In addition, we will publish the updated charter which will comprehensively address and delineate the ITOC's information technology investment management authority, responsibilities, and functions. The estimated completion date is January 2022.

OIG Recommendation 3: Keep the language from the April 2019 charter, or include similar language in its new charter, requiring the NCUA ITOC to provide a rated and ranked listing of all OPI-proposed projects to the Board, highlighting those that are statutorily or legally required.

1775 Duke Street – Alexandria, VA 22314-6113 – 703-518-6320

Page 2

Management Response: Management concurs. We will keep the language from the current draft ITOC charter and will add a comprehensive list of all information technology investments. In addition, the ITOC will detail the investments which are and are not recommended for funding in its funding request submissions to the NCUA Board. This practice will begin with the 2022-2023 budget process.

OIG Recommendation 4: Include language in the ITOC charter requiring NCUA officials to provide the ITOC minutes to the NCUA Board.

Management Response: Management concurs. We will update the ITOC charter to include the submission of ITOC minutes to the NCUA Board. The estimated completion date is January 2022.

Thank you for the opportunity to comment. If you have any questions regarding this response, please contact Shameka Sutton at (703) 548-2485 or at SSutton@ncua.gov.

1775 Duke Street – Alexandria, VA 22314-6113 – 703-518-6320

Appendix C

ACRONYMS AND ABBREVIATIONS

Acronym	Term
CIO	Chief Information Officer
CPIC	Capital Planning and Investment Control
FITARA	Federal Information Technology Acquisition Reform Act
GAO	Government Accountability Office
GAO ITIM Framework	GAO Executive Guide: Information Technology Investment Management, A Framework for Assessing and Improving Process Maturity (March 2004 Version 1.1, GAO-04-394G)
IRM	Information Resource Management
IT	Information Technology
ITIM	Information Technology Investment Management
ITOC	Information Technology Oversight Council
ITPC	Information Technology Prioritization Council
NCUA	National Credit Union Administration
NFR	Notice of Findings and Recommendations
O&M	Operations and Maintenance
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OED	Office of the Executive Director
OIG	Office of Inspector General
OPI	Office of Primary Interest
PIR	Post-Implementation Review