CREDIT UNION COMMISSION

Audit Committee Meeting

Credit Union Department Building
914 East Anderson Lane
Austin, Texas 78752

Thursday, July 17, 2025
1:00 p.m.

* * * AGENDA * * *

This meeting of the Texas Credit Union Commission's Audit Committee will be held at the Credit Union Department Building at 914 E. Anderson Ln., Austin, Texas 78752 and is open to the public. Only onsite testimony will be allowed; however, the meeting will be transmitted live through a link on the Department's webpage at www.cud.texas.gov on the day of the meeting, July 17, 2025 at 1:00 p.m.

An electronic copy of the agenda is now available at www.cud.texas.gov under Credit Union Commission, Commission Meetings, along with a copy of the meeting materials. A recording of the meeting will be available after July 17, 2025. To obtain a recording, please contact Joel Arevalo at 512-837-9236.

Public comment on any agenda item or issue under the jurisdiction of the Credit Union Commission Audit Committee is allowed. Unless authorized by a majority vote of the meeting quorum, the comments of any persons wishing to address the Commission will be limited to no more than ten (10) minutes.

The Committee may discuss and/or take action regarding any item on this agenda.

TAB		PAGE
C.	Discussion of the FY 2025 Internal Audit Report and Possible Vote to Recommend that the Commission Accept the Report and Authorize its Submission to the State Auditor's Office	**11**
D.	Discussion of and Possible Vote to Take Action on the FY 2026 Internal Audit Plan	**36**

Adjournment

Note: This is a meeting of the Audit Committee (Committee) of the Texas Credit Union Commission (Commission); however, there may be other members of the Commission attending this meeting. Since there might be a quorum of the Commission, it is being posted as a meeting of the entire Commission.

Executive Session: The Committee may go into executive session (close its meeting to the public) on any agenda item if appropriate and authorized by the Open Meetings Act, Texas Government Code, Chapter 551.

Meeting Recess: In the event the Committee does not finish deliberation of an item on the first day for which it was posted, the Committee might recess the meeting until the following day at the time and place announced at the time of recess.

Meeting Accessibility: Under the Americans with Disabilities Act, the Texas Credit Union Commission will accommodate special needs. Those requesting auxiliary aids or services should notify Joel Arevalo, Credit Union Department, 914 East Anderson Lane, Austin, Texas 78752, (512) 837-9236, as far in advance of the meeting as possible.


A.

A. CALL TO ORDER

TEXAS CREDIT UNION COMMISSION

AUDIT COMMITTEE MEETING

Committee Members

- ***Beckie Stockstill Cobb***
- ***Cody Huggins***
- ***David Bleazard***
- ***Jim Minge, Ex-Officio***

Legal Counsel

- ***Karen L. Miller***

Credit Union Department Staff

- ***Michael S. Riepen***
- ***Robert W. Etheridge***
- ***Joel Arevalo***
- ***Brenda Medina***
- ***Isabel Velasquez***

B.

B. APPROVE MINUTES OF THE JULY 18, 2024, AUDIT COMMITTEE MEETING

A draft copy of the minutes from the July 18, 2024 Committee meeting is located under **TAB B**.

RECOMMENDED ACTION: The Department requests that the Committee approve the minutes as presented.

RECOMMENDED MOTION: I move that the minutes of the Committee's July 18, 2024 meeting be approved as presented.

CREDIT UNION COMMISSION AUDIT COMMITTEE MEETING MINUTES
Credit Union Department Building
914 East Anderson Lane, Austin, Texas

July 18, 2024

A. CALL TO ORDER – Chair Kay Swan called the meeting to order at 1:00 p.m. in the conference room of the Credit Union Department Building, Austin, Texas, pursuant to Chapter 551 of the Texas Government Code, and declared that a quorum was present. Other members present included Liz Bayless, and Ex-officio Jim Minge. Committee member David Bleazard was not present due to a schedule conflict. Staff members in attendance were Michael S. Riepen, Commissioner, Karen Miller, General Counsel who will serve as legal counsel for the Committee at this meeting, and Joel Arevalo, Director of Information and Technology. Chair Swan appointed Isabel Velasquez as recording secretary. The Chair inquired and the Commissioner confirmed that the notice of the meeting was properly posted with the Secretary of State **(June 20, 2024, TRD#2024003653)**.

- **INVITATION FOR PUBLIC INPUT FOR FUTURE CONSIDERATION** – Chair Swan invited public input for future consideration by the committee. There was none.
- **ACKNOWLEDGE GUESTS** – Chair Swan acknowledged Internal Auditor, Daniel Graves and Associates from Weaver and Tidwell, L.L.P.

B. RECEIVE MINUTES OF PREVIOUS MEETING (August 10, 2023) – Mrs. Bayless moved to approve the minutes of August 10, 2023, as presented. Mrs. Swan seconded the motion, and the motion was unanimously adopted.

C. DISCUSSION OF AND POSSIBLE VOTE REGARDING 2024 INTERNAL AUDIT REPORT. Mrs. Swan explained that in August 2023 the

Commission approved an Internal Audit Charter and Plan, reviewing different high risks operations in successive years. An internal audit has been conducted for FY 2024 of the Department's examination process. Mrs. Swan called on Internal Auditor, Daniel Graves from Weaver and Tidwell, L.L.P., who introduced Michael Karnes, Manager and Connie Kang, Senior who worked on the audit. Mr. Graves reported to the Committee that they have completed the internal audit plan for the current year apart from one report and this is because guidance on that report has not come out yet. Furthermore, he explained that the first audit completed as a part of the three-year plan was the audit of examinations, being one of the most significant processes that the Commission completes and functions. Furthermore, he reported that this audit received a "Strong" for all objectives.

After a short discussion, Mrs. Bayless moved that the Committee recommends that the Commission approve the FY 2024 Internal Audit and its Submission to the State Auditor's Office. Mrs. Swan seconded the motion, and the motion was unanimously adopted.

D. DISCUSSION OF AND POSSIBLE VOTE TOTAKE ACTION ON THE FY 2025 INTERNAL AUDIT PLAN. Mrs. Swan reported that in August 2023, the Commission approved an Internal Audit Charter and Plan, reviewing different high risks operations in successive years. The plan is to focus on the Information Technology Services and Enforcement Administration for FY 2025.

After a brief discussion, Mrs. Bayless moved that the Committee recommend that the Commission approve the FY 2025 Internal Audit Plan. Mrs. Swan seconded the motion, and the motion was unanimously adopted.

E. NEXT COMMITTEE MEETING – Chair Swan reminded everyone that, if necessary, the next meeting of the Committee would be tentatively scheduled for Thursday, November 7, 2024.

ADJOURNMENT – There being no further business for the Committee, Chair Swan adjourned the meeting at 1:15 p.m.

_____	_____
Kay Swan	Isabel Velasquez
Chair	Recording Secretary

Distribution:

Legislative Reference Library

C.

C. DISCUSSION OF THE FY 2025 INTERNAL AUDIT REPORT AND POSSIBLE VOTE TO RECOMMEND THAT THE COMMISSION ACCEPT THE REPORT AND AUTHORIZE ITS SUBMISSION TO THE STATE AUDITOR'S OFFICE

BACKGROUND: In August of 2023 the Commission approved an Internal Audit Charter and Plan, reviewing different high risks operations in successive years. An internal audit has been conducted for FY 2025 with a focus on Information Technology Services and Enforcement and follow up on the 2024 focus, Administration of the Credit Union Department's examination process.

RECOMMENDED ACTION: Staff recommends to the Committee that they review and accept the Internal Audit Report for FY 2025.

RECOMMENDED MOTION: The Committee recommends that the Commission approve the FY 2025 Internal Audit Report and its submission to the State Auditor's Office.

Texas Credit Union Department

IA #01-2025 Internal Audit
Over Information Technology Services Department's IT General Controls Processes
June 20, 2025

CONTENTS

Commissioners of the Texas Credit Union Department
914 E Anderson Lane
Austin, TX 78752

This report presents the results of the internal audit procedures performed for Texas Credit Union Department (CUD) during the period February 1, 2025, through June 9, 2025, relating to the Information Systems and Technology Department (ISTD) IT General Control (ITGC) processes.

The objectives of the internal audit were to evaluate the design and effectiveness of Texas Credit Union Department's ISTD processes as follows:

A. Determine whether internal controls over Information Systems and Technology Department are designed to ensure that consistent processes are implemented and designed appropriately to address the risks within the associated sub-processes and to ensure effective operations.
B. Ensure that controls over selected critical processes within Texas Credit Union Department Information Systems and Technology Department are operating efficiently and effectively.

To accomplish these objectives, we conducted interviews and walkthroughs with ITS personnel to gain an understanding of the current processes in place, examining existing documentation, and evaluating internal controls over the processes. We evaluated the existing policies, procedures, and processes in their current state. Our coverage period was from August 1, 2023, through April 14, 2025.

The following report summarizes the findings identified, risks to the CUD, and recommendations for improvement and Management responses.

Weaver and Tidwell, L.L.P.

WEAVER AND TIDWELL, L.L.P.

Austin, Texas
June 20, 2025

Texas Credit Union Department

Internal Audit Report over IT Services Department's IT General Control Processes

June 20, 2025

Background

The Information Systems and Technology Department (ISTD) at Texas Credit Union Department (CUD) provides information technology services and supports the CUD through a wide range of activities, including end user support services, applications support, security administration, managing vendor service providers, and database administration. The ISTD utilizes the Texas Department of Information Resources (DIR) to assist with activities such as system procurement, support, and vendor management. Additionally, the ISTD utilizes a third-party IT services provider, Vintage IT Services, to assist with server maintenance and network/computer support.

Audit Objective and Scope

The scope of the internal audit included an evaluation of the CUD's ISTD to determine whether IT General Controls (ITGC) are in place to ensure that the IT processes are efficient and effective, mitigate risks related to safeguarding information, and manage data integrity of systems. We reviewed the CUD's policies and procedures in place to mitigate technology risks. The scope included an evaluation of the processes and procedures currently in place and are anticipated to remain in place in the future. Key functions and sub-processes reviewed included:

- User Administration
- Change Management
- Backup and Recovery
- Physical Access
- Vendor Management
    - Third Party Monitoring
    - Review of SOC Reports

The in-scope systems included:

- Active Directory
- CTERA
- ACT + Supporting Infrastructure (SQL Server and Windows Database)
- MERIT NCUA
- CAPPS (Financial and Human Resources modules)

Our procedures were designed to ensure relevant risks were covered and assessed the following:

<u>User Administration</u>

- Password parameters (e.g., password minimum length and complexity, expiration, account lockout) were configured to comply with industry standards.
- Administrative access to systems was authorized and appropriately restricted.
- New user accounts and changes in access were appropriately approved, and access was established as requested.
- Access reviews were performed to confirm access rights and detect inappropriate access to systems.

- Terminated personnel's system access was removed or deactivated in a timely manner.
- Generic/service accounts had an appropriate business purpose and knowledge for the credentials was limited to appropriate personnel.

Change Management

- Application and database changes were tested and approved prior to migration to production.
- Access to migrate application changes to production was limited to appropriate personnel.
- Developers do not have access to migrate changes to production.

Backup and Recovery

- Database backups were scheduled.
- The outcome of backup operation was monitored and issues resolved.
- Physical access to the CUD on-site server room was restricted to authorized personnel.

Monitoring Vendors

- Monitoring activities were performed to ensure actions performed by third party IT vendors were reviewed and approved for appropriateness.
- Applicable SOC reports were reviewed annually to ensure alignment with the CUD control environment.

Our procedures included interviewing key ISTD personnel with responsibilities in managing and/or monitoring the IT services, examining existing documentation, reviewing responses to questionnaires completed by Management, and evaluating the internal controls over the applications in scope. Our coverage period was from August 1, 2023, through April 14, 2025 for the purpose of testing activities where samples of populations were required, otherwise point-in-time testing occurred**.**

Texas Credit Union Department

Internal Audit Report over IT Services Department's IT General Control Processes

June 20, 2025

Executive Summary

Through inquiry, the completion of questionnaires, and evaluation of internal control design and effectiveness, we identified nine findings. The list of findings includes those items that have been identified and are considered to be non-compliance issues with documented Texas Credit Union Department policies and procedures, rules and regulations required by law, or where there is a lack of procedures or internal controls in place to cover risks to the CUD. These issues could have significant financial or operational implications.

A summary of our results, by audit objective, is provided in the table below. *See the Appendix for an overview of the Assessment and Risk Ratings*.

Overall Assessment		**Unsatisfactory**
Scope Area	**Result**	**Rating**
Objective A: Determine whether internal controls over Information Systems and Technology Department are designed to ensure that consistent processes are implemented and designed appropriately to address the risks within the associated sub-processes and to ensure effective operations.	Out of 12 expected IT General Controls at Texas Credit Union Department, six controls were designed appropriately for all in-scope applications. For the remaining six controls, opportunities exist to strengthen the process and control environment for at least one in-scope application, including: • Developing comprehensive IT policies over access provisioning, change management, and user access reviews • Revoking terminated user access to in-scope applications in a timely manner • Performing a periodic user access review for the Active Directory, ACT, and MS365 systems and applications • Performing a periodic user access review for privileged access within the MERIT application • Requesting, reviewing, approving, and implementing changes to the ACT database • Monitoring backup job operations to detect failed backup jobs for ACT	**Unsatisfactory**

Scope Area	Result	Rating
Objective B: Ensure that controls over selected critical processes within Texas Credit Union Department Information Systems and Technology Department are operating efficiently and effectively.	For five of 12 expected IT General Controls at Texas Credit Union Department, the processes implemented to perform the controls across all in-scope applications were not consistently executed as designed. Test procedures performed identified the following findings: • Configured password requirements in Active Directory did not meet the requirements of the Texas Department of Information Resources Security Control Standards Catalog over the enforcement of password complexity rules • Documentation of access approval for new users to ACT and CAPPS was not consistently available • A secondary user access review was not performed to validate a reviewer's own access • Segregation of privileged access between the ACT production and development environments was not consistently implemented • ACT backup job failures were not investigated or remediated	**Unsatisfactory**

Conclusion

Based on our evaluation, CUD had some procedures, practices, and controls in place to mitigate risks within the applications in scope. We identified opportunities to strengthen the processes through the development and implementation of formal policies and procedures, implementing new processes, and consistently executing controls throughout ISTD.

These improvements include:

- Developing comprehensive IT policies and procedures to standardize IT processes as provided policies did not include all control areas reviewed during the evaluation.
- Reviewing and approving all existing policies annually to ensure that policies are up to date and are reflective of current processes and requirements.
- Enabling complexity settings for Active Directory passwords to ensure difficult and hard to guess passwords.
- Removing inappropriate access to systems (including access for terminated personnel) to ensure only appropriate personnel have access. For terminations, a process should be put in place to ensure that IT personnel are notified timely of terminated individuals and for access provisioning a process should be put in place so that approvals are formally documented before access is granted., the CUD should define and implement formal periodic access reviews to ensure system access rights remain appropriate and current for in-scope applications and supporting database servers.

- Investigating and identifying a comprehensive listing of MERIT NCUA users with access to the "Admin Portal" and ensure that access is limited to appropriate personnel in line with the principle of least privilege.
- Monitoring and revoking third-party access to systems when not in use.
- Segregating administrator access to development and production environments for ACT to ensure all changes are not forgoing appropriate oversight before implementation.

Detailed Procedures Performed, Findings, Recommendations and Management Response

Detailed Procedures Performed, Findings, Recommendations and Management Response

Our procedures included interviewing key ISTD personnel with responsibilities in managing and/or monitoring the IT services, examining existing documentation, reviewing responses to questionnaires completed by Management, and evaluating the internal controls over the process.

Objective A: Design of Internal Controls

Determine whether internal controls over Information Systems and Technology Department are designed to ensure that consistent processes are implemented and designed appropriately to address the risks within the associated sub-processes and to ensure effective operations.

Procedures Performed: We interviewed key ISTD personnel with responsibilities in managing and/or monitoring the IT services, examined existing documentation, reviewed responses to questionnaires completed by Management, and evaluated internal controls to gain an understanding of the current ISTD processes for security administration, change management, IT operations, and monitoring of third-party IT providers. We documented our understanding of the processes and whether controls over the following critical sub processes existed:

Security Administration
- Authentication and Passwords
- Privileged Access
- Access Provisioning/Revocation
- Access Reviews
- Non-Individual Accounts

Change Management
- Segregation of Duties (SOD)
- User Acceptance Testing (UAT)
- Change Approvals

IT Operations
- Backup and Recovery
- Physical Security

Vendor Management
- Third Party Monitoring
- SOC Report Review

Results: Internal Audit expected a total of 12 controls to be in place over the selected systems. Through our evaluation of the CUD control environment, Internal Audit identified a total of seven controls that were appropriately designed.

Process Area	Expected Controls Coverage	Actual Controls Cover Coverage	Findings Identified
IT General Controls			
Security Administration	6*	3	1, 2, 3, 4, 6, 7
Change Management	3*	1	4, 5, 8
IT Operations	3	2	4, 9
Vendor Management	1	1	
Total	**12**	**7**	**9**

* includes one control applicable to two process areas

All (Security, Change Management, IT Operations, Vendor Management):

Finding 1 – High – Access Reviews

The requirement for formal periodic access reviews was not defined in Texas Credit Union Department policies and procedures. Further, formal periodic reviews were not performed to ensure system access rights remain appropriate and current for the following in-scope applications MERIT NCUA, Microsoft 365 Government, Active Directory, ACT and their supporting servers, tools, and databases where applicable.

Recommendation: Management should perform, at a minimum, access reviews annually. Teams performing the review should have the necessary knowledge of access rights and should maintain appropriate documentation including all relevant approvals, system listings, and results of the review as well as evidence of the method used to generate the access listings used in the review. For access modifications identified during the reviews, a post-validation assessment should be documented to verify that access changes were addressed completely and timely. In addition, secondary reviews should be performed to evaluate the appropriateness of the reviewer's access for instances in which the reviewer maintains privileges to the environment.

Management Response: Management agrees that current policy or procedures specifically addressing access reviews does not detail the specific information and processes noted in the finding. We will conduct a review of applicable policies and propose amendments or new policies and procedures to ensure these periodic reviews are performed.

Responsible Party: Director of Information Technology
Implementation Date: July 2025

Finding 2 – High – Access Revocation

Management was unable to provide a complete list of terminated employees from the HR system to Internal Audit. Consequently, Internal Audit was unable to perform comprehensive testing procedures to verify that terminated individuals no longer retain access to two key CUD systems. Without accurate and comprehensive termination data, the organization cannot effectively validate that access for former employees has been revoked in a timely manner, increasing the risk of unauthorized access to critical Credit Union Department (CUD) systems. This gap may lead to potential data exposure, misuse of system privileges, or noncompliance with regulatory requirements related to access management.

Recommendation:

Management should ensure that a complete and regularly updated listing of terminated employees is maintained and readily available from the HR system.

Management Response: The current HR system (CAPPS) is owned by the Texas Comptroller of Public Accounts. The system does not contain a report that can be generated ad hoc. Management will request a customized report for the Department that can be generated on demand through the Business Objects Core Application.

Responsible Party: Staff Services Officer
Implementation Date: July 2025

Finding 3 – High – Access Revocation

To compensate for a lack of terminated employees listing, Internal Audit selected a sample of four users with an account that was disabled during the period of the audit from a population of users for ACT and CAPPS. Internal Audit requested the documentation that supported the accounts being disabled to ensure that access was removed timely from when the HR notifications were sent.

All four sampled terminations lacked adequate support for timely access removal; either documentation was missing, or access was not revoked in a timely manner. For two of the four, the provided email evidence indicated that access remained active for between 20 and 71 days after the employee's termination date. Management should implement controls to ensure that access for terminated employees is consistently removed in a timely manner. The details are as follows:

CAPPS (FIN/HR) – 2 Users - Access Removal Dates:

1. May 7, 2024 (No evidence provided)
2. January 24, 2025 (No evidence provided)

ACT – 2 Users – Access Removal Dates:

3. September 20, 2024 (term date was August 29, 2024, 20 days after termination)
4. July 11, 2024 (term date was April 30, 2024, 71 days after termination)

Recommendation: Upon termination, Management should ensure that an appropriate process is in place to notify IT teams of the departure. Based on the termination notification, teams should initiate and complete the access revocation process in a timely manner. User accounts that are included in the termination notification should be disabled/deleted based on access removal instructions. Management should ensure that access for the four terminated employees that retained access to CAPPS and ACT has been disabled throughout all in-scope systems and perform a look back analysis to ensure no inappropriate actions were performed.

Management Response: Management agrees. There is currently no consistent and repeatable process in place to notify the IT team of the departure of employees. Based on the termination notification, IT and HR teams will herein initiate and complete the access revocation process in a timely manner. User accounts that are included in the termination notification will be disabled/deleted. Management has verified that the four terminated employees in question have their accounts disabled. We have confirmed that no activity was performed by them after their separation from the agency.

Responsible Party: Director of Information Technology
Implementation Date: July 2025

Finding 4 – High – IT Policy and Procedures
Management has not developed documented policies or procedures to formally govern critical IT control areas, including password management, user access provisioning and modifications, user terminations, and change management specific to the ACT system. While an incident response and disaster recovery policy has been established, the absence of documented policies for these additional areas increases the risk of inconsistent practices, unauthorized access, inappropriate system changes, and ineffective termination of user access.

Specifically, during our audit, we identified the following:

- Formal procedures outlining the steps for provisioning, deprovisioning, and periodically reviewing user access across the applications in scope and the network were not documented.
- For ACT, there was no documented change management policy detailing change approval requirements, segregation of duties (SOD) considerations, testing protocols, or logging and monitoring of changes.

Management provided policy 105 – Password Policy, and policy 705 – Administrative and Special Access on May 22, 2025, after the completion of fieldwork procedures. Internal Audit reviewed the policies to validate met generally accepted minimum standards for the policies, but Internal Audit was unable to perform procedures to validate whether the provisions of policies 105 and 705 were enforced across in-scope systems due to the delivery of the policies after the completion of fieldwork procedures.

Recommendation:
Management should develop comprehensive and formalized policies and procedures addressing password requirements, user access provisioning/modifications, user terminations, and change management activities. Each policy should clearly define roles and responsibilities, required approvals, segregation of duties considerations, processes to be followed, and appropriate monitoring activities. Upon creation, Management should communicate these policies to relevant staff and implement routine monitoring to ensure compliance and adherence to established guidelines.

Management Response: Management agrees that comprehensive and formalized policies and procedures addressing user access provisioning/deprovisioning, user access reviews, and change management activities should and will be developed. Each policy will clearly define roles and responsibilities, required approvals, segregation of duties considerations, processes to be followed, and appropriate monitoring activities. Upon creation, Management will communicate these policies to all agency staff and implement routine monitoring to ensure compliance and adherence to the established policy and guidelines therein.

Responsible Party: Director of Information Technology
Implementation Date: June 2025

Finding 5 – High – Change Management Process
A formalized change management process has not been established. Current practices do not require that system changes be documented, independently tested, or formally approved prior to implementation. As a result, key control activities necessary to ensure changes are appropriately authorized and executed in a controlled manner have not been designed.

Recommendation:
Management should design and implement a formal change management process that includes requirements for documenting all system changes, conducting independent testing, and obtaining documented approvals prior to deployment into the production environment. The process should also incorporate controls to ensure proper segregation of duties, with different individuals responsible for development, testing, and approval of changes.

Management Response: Management agrees that while the Department has change management guidelines, a formalized policy nor a procedure have been implemented. The Department will design and implement a formal change management process that includes requirements for documenting all system changes, conducting independent testing, and obtaining documented approvals prior to deployment into the production environment. The process should also incorporate controls to ensure proper segregation of duties, with different individuals responsible for development, testing, and approval of changes.

Responsible Party: Director of Information Technology
Implementation Date: July 2025

Objective B: Effectiveness of Internal Controls

Ensure that controls over selected critical processes within Texas Credit Union Department Information Systems and Technology Department are operating efficiently and effectively.

Security Administration

1. **Administrative/Elevated Access**

Procedures Performed: We obtained and reviewed a listing of accounts with administrator/elevated access to selected applications to verify that access was appropriate based on the individual's job title and inquiries with Management. Inquired that access to the non-individual accounts were appropriate based on business justification and access to the account.

Results: Management could not identify the roles in MERIT NCUA that allow users to perform administrative functions. Additionally, access to generic IDs with elevated access by vendor service providers was not appropriately monitored, nor was access disabled when not in use.

Finding 6 – High – Administrative/Elevated Access
Management was not able to identify a list of individuals with administrative access in MERIT NCUA. As such, Internal Audit was not able to conclude on the appropriateness of administrative access. It is critical that Management identify the roles and permissions that allow users to access the "admin portal" in MERIT.

Recommendation: Management should ensure that all elevated and administrative roles be identified by key system stakeholders to ensure access is limited to appropriate personnel.

Management Response: Management agrees. We were not aware that we do have the ability to access NCUA's OKTA Portal at the time the request was made. We have since learned that we do have access to the OKTA Admin Portal and could review the users, their roles and applications they had access to. A new policy and/or procedures will be drafted relative to use of the MERIT system with the Examination group.

Responsible Party: Network Specialist, and Director of Examinations
Implementation Date: July 2025

2. **New/Modified User (Access Provisioning)**

Procedures Performed: We selected a sample of eight new and modified users during the audit period for ACT, MERIT NCUA, and CAPPS (FIN/HR) and CTERA. For each of the samples selected, we reviewed documentation to verify that requests were created and approved by Management (as needed). We also verified that for new and modified user-access, the access granted was commensurate with the request. No new access was identified for Active Directory (admins) or Microsoft 365 Government, and as such no effectiveness testing could be performed.

Results: Security administration was not sufficiently controlled through consistent and complete documentation of access to be requested and approvals.

Finding 7 – Moderate – Access Provisioning
Six of the nine samples for ACT MERIT NCUA, and CAPPS (FIN/HR) access provisioning were either not provided, not signed off on, did not match the access requested, or did not agree with the date access was granted. Management should ensure that all access requests are documented, roles and permissions requested are specified and approved by appropriate authority, and access is provisioned as requested only after being approved. The details are as follows:

CAPPS (FIN/HR):

1. User hire date: April 25, 2024. The documentation provided was from 2020 with an approval signature from 2022. Additionally, the access requested did not match the access in the system.

ACT:

2. Administrator User created July 11, 2024. The IT ticket was completed on August 27, 2024, 36 days after the access was provisioned. Additionally, the access request form provided was not approved.
3. Standard User created June 6, 2024. The IT ticket did not specify the type of access requested to the ACT System.

MERIT NCUA:

4. User access granted September 1, 2024. Access request form was not approved.
5. User access granted November 7, 2023. Access request form was not approved.
6. User access granted June 1, 2024. Access request form was not approved, and the form did not request MERIT access.

Recommendation: Management must ensure that all new and modified access requests are documented and include: formal approval of access by the requestor's supervisor, specific requests for the access roles in the system, and the date and time of both when the request was made and when access was provisioned.

Management Response: Management agrees that there have been inconsistencies in the process in place (IT-1). Policy 705 and Procedure 138 relating to the process of access and new and terminated users will be reviewed and revised to implement these recommendations. The policy and process will be communicated, and staff will receive training. Management agrees that the system access process needs to include (IT-1 form has already been updated to include the approving manager's signature) the requestor's supervisor, the access roles being requested in the system, and the date and time of both when the request was made and when access was provisioned. The IT form will be modified to include a section where IT staff documents removal of or adjustment of the user in the system.

Responsible Party: Director of Information Technology
Implementation Date: July 2025

3. Access Reviews

Procedures Performed: Evaluated the periodic access review process for selected applications to determine if users were reviewed for appropriateness and business need, as well as if unnecessary access was identified for modification.

Results: We determined that access reviews were not performed for the period under review.

Finding 1 – High –Access Reviews

4. Terminations (Access Revocation)

Procedures Performed: Management was not able to provide Internal Audit with a list of terminated employees from CAPPS HR. As such, traditional populations and samples could not be developed and selected. The user access reports provided for ACT And CAPPS had an account disable date that allowed a limited set of four samples to be selected. Internal Audit requested the documentation that supported the accounts being disabled to ensure that access was removed timely from when the HR notifications were sent.

Results: All four of the four sampled terminations lacked adequate support for timely access removal—either documentation was missing, or access was not revoked in a timely manner. In two of the four cases, the provided email evidence indicated that access remained active for between 20 and 71 days after the employee's termination date.

Finding 2 – High – Access Revocation

Finding 3 – High – Access Revocation

Change Management

5. Change Testing, Approvals, and Emergency Changes

Procedures Performed: No formalized change Management process was in place at the time of testing. As such no substantive procedures were performed.

Results: N/A – Design Failure

Finding 5 – High – Change Management

6. Segregation of Duties

Procedures Performed: Obtained and inspected a listing of users with access to the production and development environments for ACT to verify that no segregation of duties conflicts exist.

Results: Segregation of Duties conflicts existed within the ACT development and production environment.

Finding 8 – High – Segregation of Duties
Four of five accounts granted the 'Act! Database Administrator' role in the ACT database server had access to both the ACT development and production environments.

Recommendation: Management should enforce appropriate segregation of duties between development and production environments. Specifically, individuals with development responsibilities should not have direct access to deploy changes to production. Access to production should be restricted to personnel responsible for deployment or operations, with all changes subject to formal change management processes, including review and approval. Management should review current access rights, revoke inappropriate dual access, and implement technical controls to enforce role separation.

Management Response: The database has multiple administrators at this time to enable development and conversion of old data. In addition, the administrator role was necessary for office reporting and maintaining the database. We had inadequate staff and were in the process of hiring a database administrator which occurred March of this year. As he becomes more familiar with roles, we may be able to limit users to a manager role. Use of the administrator role was necessary to successfully implement the conversion. Future changes in permissions on this database will be guided by change management policies which will be revised considering these audit findings.

Responsible Party: Director of Information Technology, and Database Administrator
Implementation Date: July 2025

IT Operations

7. Backup Configurations and Monitoring

Procedures Performed: We obtained and evaluated configuration settings for selected databases to determine if backups were configured to ensure data was appropriately backed up. Additionally, reviewed backup logs to determine if backup jobs completed according to schedule and that there were not multiple successive failures.

Results: There were a significant number of consecutive failures identified for the configured backup jobs supporting ACT Production. Furthermore, there were no alerts enabled.

Finding 9 – High – Back Up and Recovery
Through inspection of the ACT database backup audit log provided by Management, Internal Audit identified that backup procedures were not operating effectively resulting in numerous consecutive backup failures over the audit period. Specifically, the following deficiencies were identified:

- From November 11, 2024, through February 4, 2025, backups for the ACT production database failed consistently, resulting in 62 consecutive days without a successful backup.
- From February 12, 2025, through February 14, 2025, an additional 9 consecutive backup failures occurred.
- Over the past 18 months, there have been a total of 274 individual backup failures.

Backup failure notifications were not enabled, preventing timely identification and remediation of backup issues. These conditions significantly increase the risk of data loss and disruption to business operations.

Recommendation: Management should implement and enable proactive backup failure notification procedures for ACT production databases. Additionally, Management must establish a formal process to promptly review backup notifications, investigate backup failures immediately upon occurrence, and resolve all issues to ensure backups are consistently performed and data integrity is maintained.

Management Response: Management agrees with this finding. We have discovered that the backup failed because it was being done under a specific user's ID that had been removed as an administrator of the production environment because we were trying to limit the staff with administrative access. On May 21, 2025 the Database Administrator corrected the administrative rights and reset the automated backups. He also configured daily email notifications to verify that the backups complete successfully on a daily basis.

Responsible Party: Director of Information Technology, and Database Administrator
Implementation Date: July 2025

8. Physical Security

Procedures Performed: Inquired with Management regarding physical security to the on-premises server room at the CUD. Since the process in place is manual and no evidence could be provided, not additional testing was performed.

Results: The on-premises server room at the CUD is locked and can only be accessed using a key that the Director of Information Systems and Technology and the Network Specialist alone have access to. Access to the server room is limited to essential IT personnel, anyone that requires access to the server room must be escorted by the Director of Information Systems and Technology or the Network Specialist.

9. Vendor Management

Procedures Performed: Inquired with Management regarding procedures in place to ensure vendor performance is monitored and oversight performed.

Results: ACT, CAPPS, CTERA, and MERIT are managed, operated, and/or procured through another Texas State government agency that is responsible for vendor management. Active Directory and the SQL Database Servers and Windows Servers supporting ACT are managed by ISTD with the support of a vendor operating under the direct and ongoing supervision of ISTD personnel.

Appendix

The appendix defines the approach and classifications utilized by Internal Audit to assess the residual risk of the area under review, the priority of the findings identified, and the overall assessment of the procedures performed.

Report Ratings

The report rating encompasses the entire scope of the engagement and expresses the aggregate impact of the exceptions identified during our test work on one or more of the following objectives:

- Operating or program objectives and goals conform with those of the CUD
- CUD objectives and goals are being met
- The activity under review is functioning in a manner which ensures:
    - Reliability and integrity of financial and operational information
    - Effectiveness and efficiency of operations and programs
    - Safeguarding of assets
    - Compliance with laws, regulations, policies, procedures, and contracts

The following ratings are used to articulate the overall magnitude of the impact on the established criteria:

Strong	The area under review meets the expected level. No high risk rated findings and only a few moderate or low findings were identified.
Satisfactory	The area under review does not consistently meet the expected level. Several findings were identified and require routine efforts to correct, but do not significantly impair the control environment.
Unsatisfactory	The area under review is weak and frequently falls below expected levels. Numerous findings were identified that require substantial effort to correct.

Risk Ratings

Residual risk is the risk derived from the environment after considering the mitigating effect of internal controls. The area under audit has been assessed from a residual risk level utilizing the following risk Management classification system.

High

High risk findings have qualitative factors that include, but are not limited to:

- Events that threaten the CUD's achievement of strategic objectives or continued existence
- Impact of the finding could be felt outside of the CUD or beyond a single function or department
- Potential material impact to operations or the CUD's finances
- Remediation requires significant involvement from senior CUD Management

Moderate

Moderate risk findings have qualitative factors that include, but are not limited to:

- Events that could threaten financial or operational objectives of the CUD
- Impact could be felt outside of the CUD or across more than one function of the CUD
- Noticeable and possibly material impact to the operations or finances of the CUD
- Remediation efforts that will require the direct involvement of functional leader(s)
- May require senior CUD Management to be updated

Low

Low risk findings have qualitative factors that include, but are not limited to:

- Events that do not directly threaten the CUD's strategic priorities
- Impact is limited to a single function within the CUD
- Minimal financial or operational impact to the organization
- Require functional leader(s) to be kept updated, or have other controls that help to mitigate the related risk

D.

D. DISCUSSION OF AND POSSIBLE VOTE TO TAKE ACTION ON THE FY 2026 INTERNAL AUDIT PLAN

BACKGROUND: In August of 2023 the Commission approved an Internal Audit Charter and Plan, reviewing different high risks operations in successive years. The Internal Audit plan is attached. The plan is to focus on Payroll for FY 2026

RECOMMENDED ACTION: Staff recommends to the Committee that they review and accept the Internal Audit Plan for FY 2026.

RECOMMENDED MOTION: The Committee recommends that the Commission approve the FY 2026 Internal Audit Plan.

July 2025 Commissioner's Meeting
Internal Audit Status Report
As July 3, 2025

Weaver and Tidwell, LLP (Weaver) is the outsourced internal auditor of the Texas Credit Union Department (CUD). The Weaver engagement team is led by Daniel Graves, Partner.

Based on the Annual Internal Audit Plan approved by the Commissioners in August, we have completed the audit plan for fiscal year 2025.

Fiscal Year 2025 Internal Audit Plan

The FY 2025 Internal Audit Plan includes an internal audit and an annual internal audit report. The table below includes the status and progress of each portion of the plan.

2025 Internal Audits		
Internal Audit	**Description**	**Status**
Internal Audit over IT General Controls	The IT General Controls internal audit was completed on June 20, 2025. We will perform follow-up procedures over findings identified in the current year's audit in the fiscal year 2026 audit plan.	Completed
2025 Annual Audit Report		
Annual Audit Report	Internal Audit will prepare the annual internal audit report in compliance with the Texas Internal Audit act. Guidance for the report is issued by the State Auditor's Office in early August of each year. It is due to the State Auditor's Office, the Legislative Budget Board and the Governor's Office by November 1, 2025. Included with this report is the proposed internal audit plan for fiscal year 2026. This plan is consistent with the risk assessment and 3-year plan we have previously presented.	August 2025

Daniel Graves

Daniel Graves, CPA, Internal Auditor
Partner
Weaver and Tidwell L.L.P.

Credit Union Department
Proposed FY 2026 Internal Audit Plan
As of July 2025

Audit Area	Risk Rating	Summary Procedures
2026 Planned New Internal Audits		
Payroll	High	Internal Audit will include an evaluation of risks and internal controls in place related to the Credit Union Department's Payroll Management practices. Activities to be evaluated will include Timekeeping and Approval, Payroll Processing, Payroll Taxes, Compliance Reporting, Voluntary Deductions, and Accrued Leave.
2026 Planned Internal Audit Follow-up		
IT General Controls	High	Internal Audit will perform follow-up procedures on 2025 Internal Audit findings to ensure corrective action has been taken.
2026 Planned Annual Requirements		
Project Management	NA	Track overall internal audit procedures, coordinate audit activities, and reporting to management.
Update Risk Assessment	NA	Perform required annual update of risk assessment.
Annual Board Reports	NA	Prepare and submit required Annual Internal Audit Report and reports to the Audit Committee of internal audit activities.

Texas Credit Union Department
Proposed Internal Audit Plan
August 2023

Audit Area	Risk Rating	Summary Procedures	Audit Focus	Estimated Hours
2024 Planned New Internal Audits				
Enforcement Administration	High	Internal Audit will include an evaluation of risks and internal controls in place related to the Credit Union Department's examination processes. Examination areas to be evaluated will include the Complaints Processing, Investigations, Litigation, Remedial Exams, Orders and Prohibitions, Fines and Penalties, Compliance Monitoring, and Appeals.	Internal Audit	250
2024 Planned Annual Requirements				
Project Management	NA	Track overall internal audit procedures, coordinate audit activities, and reporting to management.	Project Management	15
Update Risk Assessment	NA	Perform required annual update of risk assessment.	Policy Compliance	15
Annual and Quarterly Board Reports	NA	Prepare and submit required Annual Internal Audit Report and quarterly reports to the Audit Committee of internal audit activities.	Policy Compliance	20
		Total 2024 Internal Audit Estimated Hours		**300**

Audit Area	Risk Rating	Summary Procedures	Audit Focus	Estimated Hours
2025 Planned New Internal Audits				
Information Technology Services	High	Internal Audit will include an evaluation of risks and internal controls in place related to the Credit Union Department's Information Technology practices. Activities to be evaluated will include Network Operations, Help Desk, Change Management, Software Maintenance, Software Licensing and Usage, Monitoring Third Party Providers, and Project Management.	Internal Audit	200
2025 Planned Internal Audit Follow-up				
Enforcement Administration	High	Internal Audit will perform follow-up procedures on 2024 Internal Audit findings to ensure corrective action has been taken.	Follow-up	50
2025 Planned Annual Requirements				
Project Management	NA	Track overall internal audit procedures, coordinate audit activities, and reporting to management.	Project Management	15
Update Risk Assessment	NA	Perform required annual update of risk assessment.	Policy Compliance	15
Annual and Quarterly Board Reports	NA	Prepare and submit required Annual Internal Audit Report and quarterly reports to the Audit Committee of internal audit activities.	Policy Compliance	20
		Total 2025 Internal Audit Estimated Hours		**300**

Texas Credit Union Department
Proposed Internal Audit Plan
August 2023

Audit Area	Risk Rating	Summary Procedures	Audit Focus	Estimated Hours
2026 Planned New Internal Audits				
Payroll	High	Internal Audit will include an evaluation of risks and internal controls in place related to the Credit Union Department's Payroll Management practices. Activities to be evaluated will include Timekeeping and Approval, Payroll Processing, Payroll Taxes, Compliance Reporting, Voluntary Deductions, and Accrued Leave.	Internal Audit	200
2026 Planned Internal Audit Follow-up				
Enforcement Administration	High	Internal Audit will perform follow-up procedures on 2024 Internal Audit findings to ensure corrective action has been taken.	Follow-up	50
Information Technology Services	High	Internal Audit will perform follow-up procedures on 2025 Internal Audit findings to ensure corrective action has been taken.	Follow-up	
2026 Planned Annual Requirements				
Project Management	NA	Track overall internal audit procedures, coordinate audit activities, and reporting to management.	Project Management	15
Update Risk Assessment	NA	Perform required annual update of risk assessment.	Policy Compliance	15
Annual and Quarterly Board Reports	NA	Prepare and submit required Annual Internal Audit Report and quarterly reports to the Audit Committee of internal audit activities.	Policy Compliance	20
		Total 2026 Internal Audit Estimated Hours		**300**

FUTURE COMMITTEE MEETING DATES

BACKGROUND: The committee meets on an "as needed" or "subject to the call of the chair" schedule. If a meeting is necessary, it would normally be held the day before a regularly scheduled commission meeting.

NEXT COMMITTEE MEETING: The next regular meeting of the Committee will be tentatively scheduled during the July 17, 2025 meeting.

ADJOURNMENT