NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FINAL AUDIT REPORT

NERC Organization Registration and Certification Program (ORCP) Audit

Date: May 2, 2023

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

To: Sonia Rocha, Senior Vice President, General Counsel and Corporate Secretary
Howard Gugel, Vice President, Compliance Assurance and Registration

From: NERC Internal Audit

Date: May 2, 2023

Subject: NERC Organization Registration and Certification Program (ORCP) Audit

****

Enclosed is Internal Audit's report as it relates to the NERC ORCP Audit.

The audit objective was to evaluate the success of the NERC ORCP in achieving its mission, the relationship between NERC and Regional Entities in implementing the ORCP, and the effectiveness of the ORCP.

Should you have any questions about this review, contact Kristin Miller at kristin.miller@nerc.net or at 404-230-4663.

CC:
Manny Cancel
Kelly Hanson
Stan Hoptroff
Mark Lauby
Justin Lofquist
Nina Jenkins-Johnston
Lonnie Ratliff
Jim Robb
Janet Sena
Jim Stuart

Note: Individuals whose names appear in bold type are management action plan owner(s).

EXECUTIVE SUMMARY

NERC Organization Registration and Certification Program (ORCP) Audit

Background

Under the NERC Rules of Procedure (ROP), Section 500, NERC has developed and implemented an Organization Registration and Certification Program to promote the reliability of the Bulk Power System (BPS) by establishing criteria and requirements for registered entities to register functions and obtain certification as a capable operator of Balancing Authority (BA), Reliability Coordinator (RC), and Transmission Operation Planning (TOP) functions.

The purpose of the Organization Registration Program is to clearly identify entities that are responsible for compliance with the FERC approved Reliability Standards. Organizations that are registered are included on the NERC Compliance Registry (NCR) and are responsible for knowing the content of and for complying with all applicable Reliability Standards.

The purpose of the Organization Certification Program is to ensure that the new entity (i.e., applicant to be a BA, RC, or TOP that is not already performing the function for which it is applying to be certified as) has the tools, processes, training, and procedures to demonstrate their ability to meet the requirements/sub-requirements of all the Reliability Standards applicable to the function(s) for which it is applying, thereby demonstrating the ability to become certified and then operational.

At the time of the audit, the NCR reflected a total of 1,710 registered entities. Of those registered entities, 107 BAs, 20 RCs, and 180 TOPs are subject to certification activities (18% of all registered entities).

Over the past few years, NERC and the Regional Entities have implemented program improvements and have launched a single registration information system, the Centralized Organization Registration ERO System (CORES).

The registration technology project was established to take the core registration functions currently managed in three systems, OATI (webCDMS), Guidance (CITS), and CRATS, and move all registration functions to a single consolidated system.

In addition, at least once every three years, an independent audit of the ORCP is performed under ROP Section 506. The last audit of NERC's ORCP program took place in 2019; it highlighted several process improvement recommendations and overall general conformance with the ROP. The 2022 ORCP audit was planned and executed under the leadership of NERC Internal Audit resources and conducted with observers from the Compliance and Certification Committee (CCC).

The audit observations and recommendations have been shared with NERC management and action plans have been developed to address process, control, and compliance observations. Furthermore, pursuant to ROP Section 506.3, NERC will post the final audit report for public viewing after presentation to the NERC Board of Trustees.

Audit Summary

The audit objective was to evaluate the success of the NERC ORCP in achieving its mission, the relationship between NERC and the Regional Entities in ORCP activities, and the effectiveness of the ORCP in ensuring that entities within geographic footprints are identified and that they appropriately perform specified reliability functions based on the requirements of mandatory NERC Reliability Standards and defined registration and certification processes.

The audit scope and approach focused on the evaluation of the following: NERC independent oversight processes and activities, NERC oversight of delegated authority to the Regional Entities, and program development and collaboration with the Regional Entities related to ROP and Appendix 5A (ORCP Manual) and 5B (Statement of Compliance Registry Criteria) changes, FERC directives, and strategic risks from changes in resource mix.

Internal Audit noted the following audit scope and procedure limitations:

- Manual records and listings, such as Excel spreadsheets and various artifacts, are developed for certification, therefore, Internal Audit could not verify that all entities on the NCR as BA, RC, and TOP were appropriately certified (reasonable assurance of completeness and accuracy of the NCR). Furthermore, per retention policies, certification and registration records are not maintained by NERC or the Regional Entities beyond six years, limiting representative sample testing to the period of 2016–2022.
- Validation of CORES user access at a registered entity level was not performed.

During the course of the audit and performance of our audit procedures, Internal Audit observed that NERC registration and certification activities are primarily administrative in nature and dependent on the Regional Entities to perform their obligations through delegated authority and role definition outlined in Appendix 5A. As a result, Internal Audit identified the following opportunities for NERC to demonstrate and increase the level of oversight of registration and certification activities in accordance with Section 500 and Appendix 5A and 5B:

- Design and implement a process that leverages information submitted by registered entities to Regional Entities, such as asset listings, and periodically analyze to the registration central source record (i.e. CORES and NCR) to ensure visibility to ongoing changes to the BPS across the respective geographic and cross-jurisdictional footprints.
- Direct participation in the ORCP with periodic review of documents and records of both registration and certification.
- Establish a process to periodically review the NCR against certifications, and incorporate associated certification reviews to ensure all BAs, RCs, and TOPs are appropriately certified.
- Establish routine outreach calls with all Regional Entities to review decisions concerning registration and certification status to ensure adherence with procedures and consistent application of defined criteria.
- Strengthen CORES system user access controls and perform periodic reviews to ensure access is commensurate with business role and job responsibility and demonstrates good cyber hygiene practices.

Internal Audit appreciates the time and consideration from both NERC registration and certification teams throughout this engagement.

In summary, management should consider our recommendations above and throughout the audit report to improve overall processes through more purposeful oversight and, application of strategic awareness of current and emerging risks to reliability and security that should be proactively managed through enterprise foundational functions of registration and certification of owners, operators, and users of the BPS.

Audit Period and Scope

The period under audit was January 1, 2020, through September 30, 2022.

The scope included the following components:

- Registration and Certification
  - Process and Oversight
  - Programs, Reviews and Handling
- Knowledge Management and Business Continuity
  - Operational Procedures
  - Record Retention
  - Training and Learning Programs
- Strategic Focus/Outreach
  - Strategy/Approach
  - Practice/Implementation Guides
- Systems/Business Applications and Information Technology General Controls (ITGCs)
  - User Access

Observation Summary

	Ratings			
Area	**High**	**Medium**	**Low**	**Total**
Registration and Certification	1	3	1	5
Knowledge Management/ Business Continuity	0	1	1	2
Strategy/ Outreach	0	0	0	0
Systems/ Business Applications/ ITGCs	0	4	0	4
Total	**1**	**8**	**2**	**11**

High/Medium/Low-Risk Rated Observations *(High, medium, and low risk observations require a management action plan)*		
Observation	**Risk**	**Rating**
Access to data and information is not leveraged to provide effective oversight.	NERC oversight does not identify entities that have a material or potential adverse impact to the reliability and security of the BPS.	High
Periodic oversight activities and routines are not formally established.	Regional Entities do not perform required registration and certification activities per the regional delegation agreement, and errors or omission in registration and certification adversely impact reliability and security.	Medium
Registration and certification activities are not performed in accordance with the ROP and/or processes.	Registered Entities perform functions without validation of the required capabilities that ensure reliability and security of operations; lack of process integrity reduces visibility to BES assets and associated compliance requirements.	Medium
Registration deactivation notification letters do not contain document retention requirements in accordance with ROP and/or process	Information or data loss to support operational decisions or disputes.	Low
Implementation of recommendations from NERC-led registration review panels are not confirmed.	Registered entities do not receive timely communication and guidance to perform required functions prior to operational activities and in compliance with Reliability Standards.	Medium
Operational processes and knowledge management is ineffective.	Registration and certification process execution and continuity is not sustainable to support integral current and future activities.	Medium
User onboarding and termination procedures for CORES access are not performed.	Access is granted to persons without a business purpose and not in compliance with existing policy and a terminated employee has remote access to the network or email system and unauthorized/malicious activity occurs.	Medium
Periodic revalidation review of user's access to CORES is not performed.	A terminated employee gains remote access to the network or email system; segregation of duties issues result if an employee retains system privileges from a previous department.	Medium
Generic user account is actively used.	Account security is compromised and unauthorized access and/or malicious activity occurs.	Medium
De-registered entities are listed as users in CORES.	Account security is compromised and unauthorized access and/or malicious activity occurs.	Medium
Required certification training was not completed and validated by the certification team lead (CTL).	Personnel are not equipped to perform certification responsibilities effectively and sustainably relevant to the current environment.	Low

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date/Responsible Person(s)	Impact
1.	**NERC Oversight** Oversight ROP sections: Section 501 1.4; 1.4.1; 3.1; 3.3; 3.3.2 Section 502 1.2 NERC Oversight Plan 2/16/21 ROP Section 507 Appendix 5B; Statement of Compliance Registry Criteria; Resolution (1 and 2)	**Access to Data and Information is not Leveraged to Provide Effective Oversight** Through inquiry with management and understanding of registration and certification processes, Internal Audit identified the following: • Asset listings provided to Regional Entities on a periodic basis to substantiate assets within registered entity footprints are not reviewed by NERC against the NCR or certification records. • Registration central repository (CORES/NCR) is not reconciled periodically with manual certification listings/records to ensure all BAs, RCs, and TOPs are appropriately certified. • Models and system diagrams are not leveraged to provide insight that the assets and systems are adequate by registration. Consistent with NERC's oversight role, the Organization Registration Program should clearly identify those entities that are responsible for compliance with the FERC approved Reliability Standards. Also, NERC shall establish and maintain the NCR of the bulk power system owners, operators, and users that are subject to approved Reliability Standards. Last, NERC and Regional Entities have identified two principles they believe are key to the entity selection process: consistency between Regional Entities and across the continent with respect to which entities are registered; and any entity deemed material to the reliability of the BPS will be registered, irrespective of other considerations. To address the second principle, the Regional Entities working with NERC will identify and register any entity they deem material to the reliability of the BPS. NERC may not identify entities that have a material or potential adverse impact to the reliability and security of the BPS without established	NERC registration will develop procedures to work with Regional Entities to identify the information collected during entity registration and confirm correct functional registration. Also, NERC registration will review each Regional Entity registration process to ensure completeness and consistency. Furthermore, NERC registration will use this and other information to confirm accuracy of NCR, Joint Registration Organization (JRO), and Coordinated Functional Registration (CFR) records and registration. NERC registration will establish processes to preserve ongoing accuracy of these records. MAP Due Date: October 31, 2023 Associate Director–Registration	High

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date/Responsible Person(s)	Impact
		oversight activities, including periodic reviews of information, data, and documentation. NERC works through collaboration with ERO Enterprise working groups. Asset listings and associated processes differ across the Regional Entities and are not periodically requested by NERC for review or analysis of respective ERO geographic or overall footprint(s). Through oversight of Regional Entities, NERC should design and implement a process consistent with Appendix 5B and leverage information, such as asset listings, that is periodically submitted by the registered entities. NERC should analyze the information and share with the Regional Entities to identify impacts to registration and certification.		
2.	**NERC Oversight** ROP Section 501, 3.3.2; Appendix 5A Appendix 5B; Statement of Compliance Registry Criteria	**Periodic Oversight Activities and Routines Are not Formally Established** During the audit process walkthroughs, NERC acknowledged they do not periodically review documents and records of both programs as an established oversight activity. Through further inspection, the following was noted: • Annual oversight was evidenced for some Regional Entities through the submission of a NERC-executed letter that outlines the reviewed scope and areas. However, supporting documentation, checklists, or evidence of review was not provided. Also, recommendations were not provided to the Regional Entity to improve processes and activities. • Periodic reviews of Regional Entity status and decisions related to certification and registration is not performed or evidenced through documentation.	NERC CA will formalize and document a certification oversight plan to include status, direct observation, periodic reviews, frequency of activities, and establish a feedback mechanism to the Regional Entities. NERC registration will formalize and document a registration oversight plan and conduct a regimen of oversight engagements with each Regional Entity to confirm accuracy of NCR, JRO, and CFR records. NERC registration to continue to confirm performance of each Regional Entity to comply with registration time lines as described in the ROP.	Medium

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date/Responsible Person(s)	Impact
		• Registration program reviews are not performed to ensure that changes in registration that involve parties to a CFR and/or JRO are updated accordingly. NERC's oversight should consist of developing and maintaining a program to oversee the ORCP activities that are delegated to the Regional Entities through the delegation agreement. Monitoring and oversight shall be accomplished through direct participation in the organization registration and organization certification programs with periodic review of documents and records of both programs. Without periodic review of documents and records, Regional Entities may not perform required registration and certification activities in accordance or consistent with the Regional Delegation Agreement, Appendix 5A defined roles and Appendix 5B compliance registry criteria as well as errors or omissions in registration and certification adversely impact reliability and security. NERC relies on the Regional Entities to perform activities completely and accurately in accordance with delegated authority and in compliance with the ROP and appendices 5A and 5B. In addition, certification monthly reviews were conducted on a limited basis for two of six Regional Entities. NERC's monitoring and oversight should include periodic and annual review of documentation for registration and certification on a determined frequency to ensure visibility into each program of responsibility by the Regional Entities. Changes to source records should be crosschecked and updated across each program area (i.e., CRFs, NCR, JROs, certifications, and certification reviews).	MAP Due Date: August 31, 2023 Director–Compliance Assurance and Certification Associate Director–Registration	

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date/Responsible Person(s)	Impact
3.	Appendix 5A; NERC roles and responsibilities: NERC (4) ROP Section 501 2.1-2.5 NCR: Section 502; 2 NERC is required to maintain all registration and certification records	**Registration and Certification Activities are not Performed in Accordance with ROP and/or Process** NERC registration and certification do not maintain records, including granting certification certificates for the Registered Entity(ies) responsible for compliance: • Three registered entities were registered as TOP and did not evidence certification. • Three registered entities were registered as a BA and did not evidence certification. • Registration of an entity for a function has continued since November 2020; operating under a conditional certification without evidence of completion of the implementation plan. • NERC certification letters or certificates were not consistently retained. NERC is required to maintain accurate registration and certification records including granting certification certificates for the Registered Entity(ies) responsible for compliance (including JRO/CFR). Conditional certification should be defined within Section 500 and Appendix 5A or another mechanism to ensure adherence to compliance with Reliability Standards and process effectiveness/consistency for exceptional situations. Registration and certification process integrity and sustainability may not be reliable and reduces visibility to BES assets and associated compliance requirements per the ROP and Reliability Standards. The activities of the program are designed to identify issues that, if not closed, could lead to unacceptable performance of the duties and responsibilities applicable to	NERC CA will formalize and document data retention expectations internally and for the Regional Entities as well as documenting oversight as part of the certification oversight plan. NERC CA will review the entities that did not evidence certification to determine whether historical decisions were appropriate and take appropriate action where the decisions were not. In addition, NERC CA will evaluate technology solutions to centralize a repository for certification records. NERC registration will develop a procedure to confirm completion of certification activities with subsequent timely accurate registration of entity. Furthermore, NERC registration and certification will initiate a joint evaluation of a technology solution for a depository of certification and registration records. MAP Due Date(s): September 30, 2023	Medium

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date/Responsible Person(s)	Impact
		the certified function. Also, in the absence of a certified RC, TOP, and/or BA for any area jeopardizes the functional relationships within and between areas specified by the Reliability Standards and may lead to the inability of registered entities to maintain compliance with standards that require performance with respect to those relationships. NERC concurred with the Regional Entity's decision not to certify in each instance for various reasons, such as the entities were performing a lesser activity; the entity was operating as a TOP while unregistered for a BA and unable to obtain certification until correction of known deficiencies; and an entity expanded into another Regional Entity's footprint. Subsequent ROP changes effective in 2021 were retroactively referenced as a basis for NERC's acceptance if these ROP/process deviations. Also, NERC did not maintain certification letters and certificates for all entities as required per document retention requirements. NERC should maintain adequate records and consider implementing an oversight activity or monitoring control to verify the required documentation is retained internally and/or by the Regional Entity as intended.	Director–Compliance Assurance and Certification Associate Director–Registration	
4.	**Registration and Certification Processing** ROP Section(s) Appendix 5A Section B.3	**Registration Deactivation Notification Letters do not Contain Document Retention Requirements in Accordance with ROP and/or Process** Through inspection of various registration types and programs (e.g., JRO, CFR), including a listing of registration deactivation and deregistration information during the period of our audit, Internal Audit identified that, of the 29 deactivation letters reviewed, none contained language related to the obligation to retain records according to the retention period.	NERC registration will modify its form letter sent to entities that have been removed from the NCR. The modification will include notification of the ERO's obligation to keep entity information as required by NERC's data retention obligations. Registration will notify those relevant previously deactivated	Low

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date/Responsible Person(s)	Impact
		NERC is required to notify the entity of the retention period in accordance with the NERC ROP to ensure records are maintained for the appropriate period after deactivation. NERC was not aware of the omission and letters were not periodically reviewed to ensure that the retention requirement was included in accordance with the ROP for the specified period after deactivation. A registered entity will not be aware of the record retention period and delete/destroy documentation required for retention by the Regional Entities and/or NERC in event of an issue and audit trail needed to ensure transfer of operational and/or compliance responsibility. NERC should update the deactivation letter template to include retention language and communicate to Regional Entities and registered entities for awareness and compliance with the ROP requirement.	entities of NERC's data retention obligations. MAP Due Date: September 30, 2023 Associate Director– Registration	
5.	**Registration and Certification Processing** ROP Section: 501 1.7 Appendix 5A; Section III D	**NERC-Led Registration Review Panel Recommendations are not Confirmed/Implemented** Review of NERC-led panel reviews identified: • Four panel reviews were conducted during the audit period and follow up was not performed with the Regional Entities to ensure registration and certification occurred. • Panel reviews are executed in isolation of the certification process. For entities that include BAs, RCs, or TOPs, NERC certification staff was not a participant in the panel. Per Appendix 5A, any required changes to the NCR resulted from the Panel decision will be initiated by the Regional Entity in accordance with the Organization Registration Process.	NERC CA will work with NERC registration to evaluate the NERC-led registration review panel procedure document, including roles and responsibilities for certification. NERC registration will update the "NERC ERO Enterprise Registration Procedure" to ensure recommendations that result from each NERC-led panel are documented and implemented in coordination with NERC certification.	Medium

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date/Responsible Person(s)	Impact
		Decisions and or actions related to registration as recommended by the review panel may not be implemented or certifications may not be performed in a timely manner. Also, entities may be registered for a function for which certification was required but not completed. A formal process to follow up on the recommendations from the NERC-led review has not been established. NERC should update the "NERC ERO Enterprise Registration Procedure," dated November 5, 2021, to include NERC-led review follow-up and provide Regional Entity oversight to ensure recommendations are implemented. In addition, when a recommendation involves a BA, RC, or TOP the procedure should include certification prior to an entity being added to the NCR.	MAP Due Date: July 31, 2023 Director–Compliance Assurance and Certification Associate Director–Registration	
6.	**Knowledge Management and Business Continuity** ROP Section(s) Section 501 - Entity Certification Appendix 5A Organization Certification Process -	**Operational Processes and Knowledge Management is Ineffective** Through inquiry with management and inspection, Internal Audit identified the following: • Certification records were manually developed and maintained by two different staff during the audit period due to organizational changes. The transition of knowledge was not evident from the prior gatekeeper of information to the current staff managing certifications. Additionally, there is not a single source record of certifications applicable to all required functions (BA, RC, and TOP). Staff rely on manual spreadsheets for tracking purposes that were created in March 2022. • The nerc.com certification site has outdated documentation, templates, and inactive links to information.	NERC CA will evaluate staff assignments for continuity of operations and document internal processes, including roles and responsibilities. In addition, NERC CA will work with the Regional Entities to update the ERO Enterprise certification processes and templates, including general clean-up of the certification webpage. NERC CA will work with NERC registration to review and document handoffs between registration and	Medium

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date/Responsible Person(s)	Impact
	Initiation 3, 3b; Reporting item 9	▪ Approximately 90% of the website documentation was posted in 2013 at a time when there were eight Regional Entities. • Although registration and certification processes are to be executed concurrently, silos exist with limited evidence of a hand-off process; key decision making documentation related to registration and certification is not maintained within CORES or Align. • Both processes rely on one key individual with limited continuity or back up. • Procedure gaps were identified to include the handling of conditional certifications, actions related to NERC-led registration review panel conclusions and recommendations, and responsibilities outlining registration and certification oversight activities. • CFR data has not been fully migrated to CORES. • Evidence was not provided of proposed certification schedules submitted from Regional Entities to NERC for review and approval. NERC did not formally approve, modify, or reject a proposed certification schedule. • Extensions for certifications outside the nine-month time line is an informal process and not evidenced through a documented approval process by all parties. The Rules of Procedure Section 501-Entity Certification states that NERC's program shall maintain process documentation and maintain records of currently certified entities. In addition, Appendix 5A states that it is NERC's role and responsibility to maintain accurate registration and certification records.	certification as necessary and evaluate a possible single technology solution. NERC registration will evaluate staff assignments for continuity of operations and document internal processes, including roles and responsibilities. Furthermore, NERC registration will document internal processes to enhance operational continuity. NERC registration will work with NERC CA to review and document process handoffs between registration and certification as necessary and evaluate a possible single technology solution (see Item 5 above). MAP Due Date(s): December 31, 2023. Director–Compliance Assurance and Certification Associate Director–Registration	

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date/Responsible Person(s)	Impact
		Process execution and continuity may not be sustainable to support integral BES activities through registration and certification. NERC relies on Regional Entities to retain registration and certification documentation, and current systems, processes, and procedures do not ensure completeness and accuracy of information. In addition, processes are not designed and implemented with validation of handoffs required between the two operational functions. NERC registration and certification functions should consider implementing a single and/or integrated automated solutions for registration and certification data and information. The data and information that support registration and certification processes should be contained or archived within the solutions or tools, such as applications, letters, certification reviews, conditional certifications, and implementation plans. In addition, operational procedures should be developed to promote consistency and continuity in process execution and support the transfer of knowledge and training in the event of staffing or organizational changes.		
7.	**NERC Registration** **IT General Controls (ITGCs)** **GTAG1:** Information Technology Controls	**User Onboarding and Termination Procedures for CORES are not Performed** Registered entities may grant permissions for access to CORES through the ERO Portal. ERO Enterprise staff may grant permissions for access to CORES through the XRM system. Current procedures used to assign roles when adding a new user or changing roles for an existing user within CORES do not require business owner approval.	NERC registration will remove ability for all IT support staff except system administrators from assigning/revoking CORES roles for Registered Entity User permissions. In addition, NERC will work with IT to publish a process for Client Services that resolves Registered	Medium

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date/Responsible Person(s)	Impact
	apply to all systems, components, processes, and data for a given organization or IT environment ITGCs ensure the proper development and implementation of applications, as well as the integrity of programs, data files, and computer operations. Employee InfoHub/Policies and Procedures/IT Department/Information Security/Information and System Access Control Policy/Access Application	Currently IT Analysts are sense-checking the email address received via a client services ticketing system for reasonableness (i.e., not obviously fake) before they effectively authorize and establish the account. However, IT Analysts are not in a position to be authorizing user access. The Application Access Policy states: • Request for application access must be recorded and available for auditing in a central location. Email storage is not sufficient to satisfy this requirement. • Application access is granted by the business owner of the application, recorded, and associated to the initial request. The Information and System Access Control Policy states that all requests for access authorization must be submitted via the Client Service ticketing system following established ticket submittal guidelines. Upon submission of a Client Service ticket, the technician working the Client Service ticket must send a corresponding email to the department manager or director to alert them of the request for access authorization. The Access Authorization Policy states: • Access to information and information systems shall be based on user need as defined by his or her job function and approved by the information owner. • Information owners must report to IT changes in information users' job functions that affect access privileges within 24 hours of the change. A separate process may have to be implemented for registered entities for CORES and another process for Regional Entity and NERC personnel for CORES and XRM.	Entity users' CORES permissions issues, including obtaining approval from CORES business owners before taking any action on modifying access. Define and publish procedure by which ERO Enterprise Staff submit requests for CORES access through the help desk ticketing system, require Business Owner approval before adding users or removing user's access to the CORES system, and ensure routing to the system administrator for granting or revocation of permissions. MAP Due Date: June 1, 2023 Associate Director–Registration Director–Enterprise Application Architecture	

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date/Responsible Person(s)	Impact
	Policy/Account Terminations Policy	Without a documented business approval process in place, user access may not be appropriate or as management intends. A process to document user access as part of initial onboarding as well as user access changes should be developed. A predetermined list of roles for each application should be documented where the business approver selects the desired role and attaches the form to a client services ticket for IT Administration to then setup the user. As CORES users are given logon credentials, a process to remove the access has not been formally documented. Without formal documentation of the termination process the user's access may not be removed timely, increasing the risk of unauthorized access. The Account Termination Procedure states the following: • Human Resources or the department manager (in the instance of a contract or intern resource) will open a "high" priority client support service request ticket immediately upon notice of termination of employment. • Although the active directory should minimize user's access, CORES and XRM user profiles should be removed as orphaned user ID's increase the risk of unauthorized activities. • Human resources or the business owner must initiate a ticket, where the requester/approver identifies the user to be removed, with the form being submitted via the Client Services ticketing system.		

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date/Responsible Person(s)	Impact
		• Lastly, ensure the ticket is routed to the System Administrator for deactivation in the CORES and/or XRM system.		
8.	NERC Registration Employee InfoHub/Policies and Procedures/IT Department/ Information Security/ Access Application Policy	**Periodic Revalidation Review of User's Access to CORES is not Performed.** Procedures for periodic review of user's access in CORES is not documented. Furthermore, Internal Audit could not verify the user review control is in place as there is no evidence of the performance for CORES or XRM. The Application Access Policy states that access reviews are required annually. Lack of a periodic review increases the risk of unauthorized access to confidential information. Implement a process to review standard and privileged access to the in-scope applications annually to validate the appropriateness and employment status of users. NERC management should obtain and maintain evidence to ensure that this control is operating as intended. The documentation should include/evidence of the following: • Completeness of a user listing (e.g., parameters used to extract all the user listings with row count generated) for the listing to be used for the periodic review. • Actions requested as a result of the review have been completed (e.g., new listing where modified access was needed).	For registered entity users, develop a programmatic certification procedure by which Regional Entity administrators, on behalf of their Regional Entity, are required to review and attest the list of users that have access to CORES. For ERO Enterprise users, certification will be implemented as part of the Identity Governance and Administration program. MAP Due Date: September 8, 2023 Associate Director–Registration Director–Enterprise Application Architecture	Medium

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date/Responsible Person(s)	Impact
		• Final signoff of the review, including the date and name of the business reviewer.		
9.	NERC Registration Employee InfoHub/Policies and Procedures/IT Department/Information Security/ Access Application Policy/Access Authorization Policy	**Generic User Account is Actively Used** Our review noted the use of a generic "WECC Registration" account within XRM/CORES. The generic account is not assigned to an individual and the account was established for ease-of-use allowing several individuals to share a user ID and password for access. Shared or generic accounts do not allow for the identification of a specific user and are a violation of NERC's Access Authorization Policy where "user access is controlled via unique user identification codes and passwords." ERO Enterprise staff must utilize unique ID's when granting permission to CORES and each user must be assigned a unique identification code and password. Shared user ids and passwords compromise account security and without having malicious intentions, users could open the company up to compromise simply by sharing login credentials with people who may be using insecure hardware**.** NERC should ensure that processes are established to detect and deter the establishment of generic accounts and use of shared passwords in accordance with the Access Authorization Policy. In addition, NERC should communicate these policy requirements to Regional Entities as recommended "cyber hygiene" practices and disable generic accounts.	All ERO Enterprise and registered entity user accounts in the XRM platform will be reviewed to determine if they are generic. All instances of generic accounts will be eliminated. An additional step will be added to the Client Services Account Approval process in which new accounts will be reviewed to confirm they satisfy account criteria and are not generic accounts. MAP Due Date: June 1, 2023 Associate Director–Registration Director–Enterprise Application Architecture	Medium

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date/Responsible Person(s)	Impact
10.	NERC Registration Employee InfoHub/Policies and Procedures/IT Department/Information Security/ Access Application Policy/Access Authorization Policy/Account Terminations Policy	**De-registered Entities are Listed as Users in CORES** Our review of a sample of CORES User Access profiles identified users associated to Registered entities which have been de-registered. All users from de-registered entities should have their access to CORES removed in a timely manner. Continued account access for these users increases the risk of unauthorized access to CORES. A process is not in place to identify users at a registered entity level and periodically validate business need for access and/or current status within the entity and/or organization. NERC should establish a process to ensure that access is removed timely for users that no longer possessing a business need or are not employed within the organization. In addition, for the sample of users identified with access as a deregistered entity, access to CORES should be immediately removed.	For registered entity users, as part of the certification process outlined in the MAP for observation 9, entity administrators will be directed to remove the entity-specific CORES entitlements from those registered entity users that are no longer affiliated with their entity. When a registered entity is de-registered in the CORES system, all CORES-specific entitlements for registered entity users to that entity will be programmatically revoked. MAP Due Date: September 1, 2023 Associate Director–Registration Director–Enterprise Application Architecture	Medium
11.	Knowledge Management/ Business Continuity Training and Learning Programs	**Required Certification Training was not Completed and Validated by the CTL** Through inquiry with management, and inspection of a sample of personnel requiring certification training the following was identified: • Of the 68 personnel training records selected, 33 (48%) certification member training records were not provided to evidence that the required training was administered.	NERC CA will document roles and responsibilities in its internal process documents, including the development and delivery of certification related training. In addition, NERC CA with work with the Regional Entities to update the ERO Enterprise certification	Low

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date/Responsible Person(s)	Impact
	ROP Section 502 2.27; Appendix 5A; Section 900; 901. Appendix 5A; pg.15 Item 3	• In addition, records did not include CTL validation of the Certification Team (CT) member's qualifications that successfully demonstrate requisite knowledge and skills with no conflicts to be a CT member. Per ROP and Appendix 5A, CT members shall have the necessary diversity in their technical training and experience to collectively represent the subject matter competencies needed to perform the evaluation of the specific function being certified. The CTL shall ensure all CT members have completed CT member training requirements as established by NERC and Non-ERO employees shall also complete the following: • CT member training record form • CT conflict of interest form • An ERO confidentiality agreement form Technical training and conflicts may not adequately equip personnel to perform certification responsibilities effectively and sustainably, relevant to the current environment. Maintenance of training records varies across the Regional Entities and oversight by NERC to ensure training is completed is not documented. In addition, certification team member training records were not validated by the CTL prior to the performance of certification and certification reviews. NERC should develop a training and learning program strategy for Regional Entities to ensure consistency across the ERO Enterprise for	processes and templates to document training expectations, including controls for verification of team member and team lead training. NERC CA to incorporate into annual oversight plan developed in observation 2, including the expectation that CTLs are trained prior to leading an engagement. MAP Due Date: December 31, 2023 Director–Compliance Assurance and Certification	

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date/Responsible Person(s)	Impact
		completion of CTL and CT member training records and validate performance of the required training has occurred. In addition, NERC certification should develop internal process documentation for roles and responsibilities of certification staff, and internal procedures that are required for consistency in program execution.		

Appendix

Audit Approach

The scope of our procedures was determined through our annual risk assessment process, discussions with members of management, and qualitative and quantitative factors identified during the audit-planning phase. The audit engagement team performed various auditing techniques described in the table below:

Technique/Test	Description
Inquiry	Questions and responses to confirm understanding and ownership of processes, risks and controls; potentially establish additional testing criteria.
Inspection	Examining records or documents indicating performance of the control activity or physically examining inventory, systems, books and records.
Observation	Looking at a process or procedure performed by others (e.g., observation of user access reviews by the Company's personnel).
Re-performance	Verifying the operational effectiveness and/or accuracy of a control.
Analytical Procedures	Evaluating information by studying plausible relationships among both financial and nonfinancial data.

Throughout our testing, Internal Audit used widely accepted audit sampling techniques. These sampling techniques allowed us to obtain audit evidence, which is sufficient and appropriate, and necessary to arrive at a conclusion on the population.

Note: The status of the management action plans will continue to be reported to the Audit/Finance Committee until the observation is successfully remediated.

Observation Ratings

In determining an observation’s risk rating (i.e., high, medium, or low), Internal Audit considers a variety of factors including, but not limited to, the potential impact, the likelihood of the potential impact occurring, risk of fraud occurring, regulatory and legal requirements, repeat observations, pervasiveness, and mitigating controls.