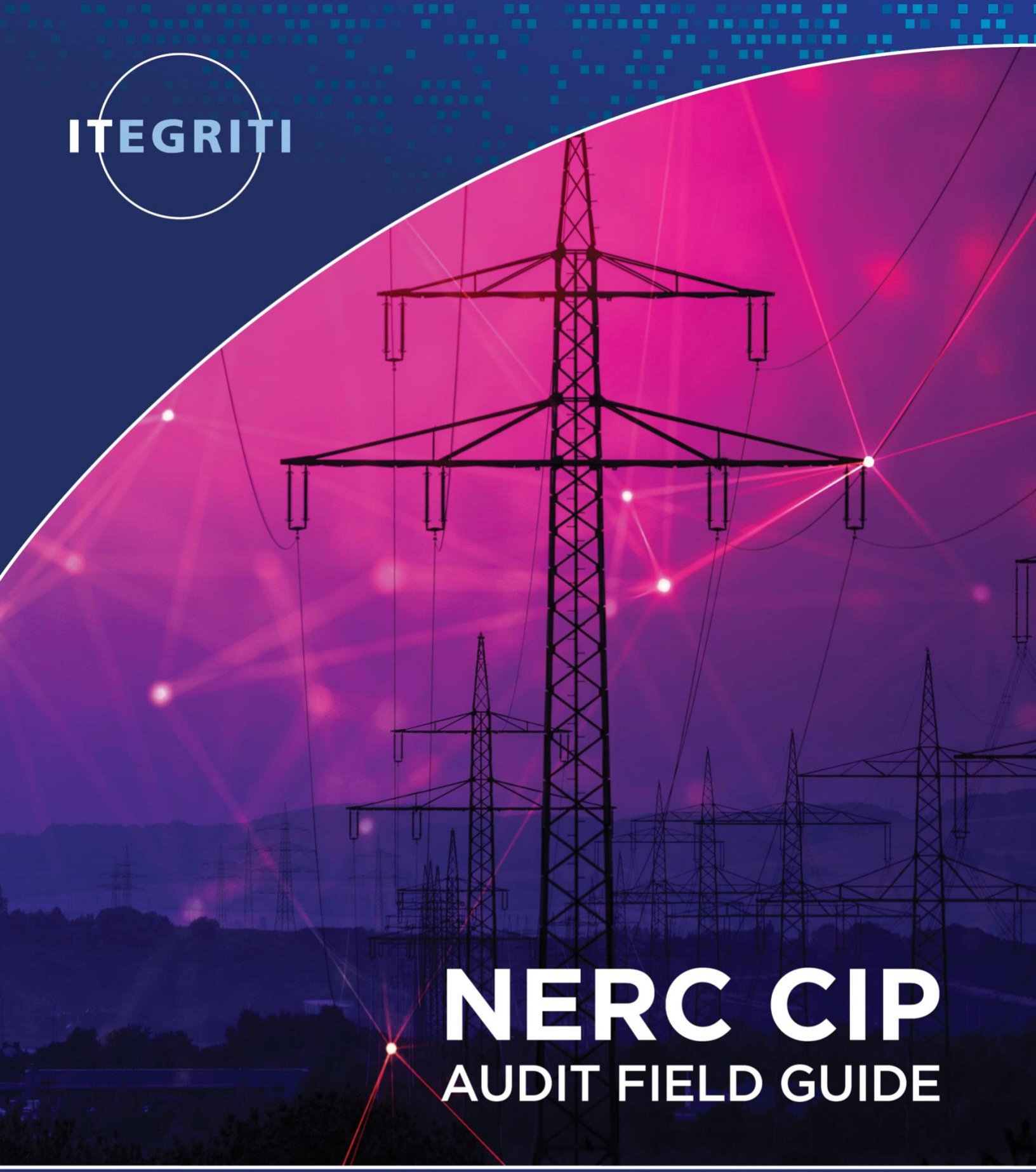
ITEGRITI



NERC CIP
AUDIT FIELD GUIDE

RELIABILITY THROUGH CYBERSECURITY RESILIENCE™

Contents

Foreword

The role we share in providing safe, reliable power is essential and rewarding, but it can be stressful. As witnessed during Texas's February 2021 power outages, the consequences can be devastating when critical infrastructure fails. We live in Houston and can provide a first-hand account of what happened when entire communities lost power for days/weeks, which in turn caused a lack of Internet, phones, heat, and water. These events, which cost approximately $200 billion, affected over four million homes and businesses.

To improve the reliability and security of the U.S. Bulk Electric System (BES), the North American Electric Reliability Corporation (NERC) created a series of critical infrastructure protection (CIP) standards, with which all U.S. BES owners and operators must comply. These standards apply to multiple components of the BES, including generation, transmission, energy management systems, and supply-chain risk management. The reliability of critical infrastructure assets is not only threatened by extreme acts of nature but also by technology mismanagement, interdependence, and cyberattacks.

Enhanced network connectivity has increased risk and susceptibility. Over the past several years, multiple cyberattacks on operational technology (OT), including Supervisory Control and Data Acquisition (SCADA) and other industrial control systems (ICSs), which monitor, control, and access operational and industrial equipment, have made national and international headlines. One approach to bolstering the security of these OT assets is through an independent review of Critical Infrastructure Protection programs.

Proper preparation for NERC audits requires dedication, planning, and a strong culture of compliance and security for REs, which can be challenging. However, NERC has worked to standardize and improve the audit process.

We first started serving NERC clients in 2006. Over the last decade, we have witnessed impactful and very positive changes, including in 2020 when NERC and the regional entities implemented audit process changes designed to protect the health and safety of participants during virtual NERC CIP audits. These audits can be stressful, but keep in mind that all participants share a common goal: to verify the RE's ability to provide reliable power by enhancing the reliability of BES cyber systems/assets, along with additional supporting assets.

This field guide, compiled using input from our team comprised of seasoned professionals advisory team members, and industry partners (with numerous years of collective compliance and cybersecurity experience), contains sound advice toward achieving positive results before, during, and after the NERC CIP audit process.

To set the stage, we begin by providing you with a brief introduction and background, along with an overview of the NERC CIP standards. The document then progresses from preparation through the actual audit, concluding with lessons learned and post-audit activities. We include recommended steps to follow, resources, and valuable references for successfully navigating the audit process throughout this field guide. We hope this asset proves beneficial and appreciate input, suggestions, and candid feedback, as we will update and improve this guide periodically.

Michael Sanchez, CEO

Sid Shaffer, Chief Delivery Officer

Dr. Thomas Duffey, Director of Cybersecurity and Compliance

ITEGRITI Corporation

1 Regulatory Background & History

We have come a long way since the initial creation of the roots for the electric power grid. Society has progressed from simply keeping the proverbial lights on, to homes and businesses filled with electronics and machines. The first well-known power outage dates back to 1965 leaving the entire northeast region without power for approximately 13 hours.

Based on the findings from this blackout, the National Electric Reliability Council was established with the goals of information dissemination, review, discussion, and assistance in resolving matters involving nine regional utility reliability organizations through voluntary cooperation. Almost a decade later, there was a subsequent New York power outage in 1977. This event led to the Department of Energy Organization Act and President Wilson's Federal Power Commission repurposing the Federal Energy Regulatory Commission (FERC), whose mission was to provide oversight and regulation of the energy sector. Following Western United States (U.S.) blackouts in 1996, a joint task force determined the need for the creation of an independent self-regulatory auditable electric reliability organization (ERO) to enforce mandatory rules for the bulk electric system (BES).

During August of 2003, weakened power lines brushing against overgrown trees caused electrical faults, but alarms did not effectively trip due to system failures attributed to impacts from the Blaster worm. Cascading events from this catalyst impacted southern Canada and eight northeastern U.S. states, leading to loss of power for approximately 50 million people. Following this major outage, what began as voluntary guidelines and standards for the electricity industry changed. The resulting Energy Policy Act of 2005 included requirements for implementing standards to improve electric grid reliability, including Critical Infrastructure Protection (CIP) standards.

This legislation, which included the Electricity Modernization Act of 2005, mandated that compliance with these standards would be mandatory and enforceable Standards, mitigating operational and cyber risks to the BES, and authorizing the creation of an ERO under the oversight of FERC. Within Order 672-A, FERC responded by certifying the North American Electric Reliability Council as the U.S. ERO. The name was changed to the North American Electric Reliability Corporation (NERC). With the assistance of eight Regional Entities (there are currently six), NERC provided enforcement of the CIP standards using audits, random inspections, voluntary self-reporting procedures, and investigations of possible violations. All bulk power system owners, operators, and users must register with NERC through the appropriate Regional Entity and comply with NERC-approved Reliability Standards

The first NERC issued standards, which became mandatory and enforceable on June 18, 2007, focused primarily on operational risk areas. However, due to the increased dependency of the electric grid on network/internet connectivity, cybersecurity-related standards soon followed. FERC issued Order 706, approving the first version of the CIP Reliability Standards, on January 18, 2008. These standards aim to ensure all relevant NERC electric entities adhere to them and adequately safeguard their assets against potential cyber threats. Since then, multiple iterations and revisions to the CIP standards have been implemented, and older versions retired. The currently enforceable NERC CIP framework includes 11 cybersecurity

standards and one (1) physical security standard (see Appendix A).

These standards mandate implementation by energy and utility companies operating BES Cyber Assets (BCAs) composing BES Cyber Systems (BCSs) to help mitigate the risk of cyberattacks and manipulation by malicious actors seeking to cause damage. Applicability of the NERC CIP standards includes all interconnected jurisdictions in North America (including regularly scheduled oversight), the Mexican state of Baja California Norte, and the majority of Canada (although enforcement and management differ.

Since these standards are mandatory, regulatory bodies provide oversight to help ensure proper adherence by the relevant entities. This oversight includes several components: Compliance Audits, Spot Checks, Self-Certifications, and Periodic Data Submittals – with audits being the primary method of regularly scheduled supervision.

2 Overview of the CIP Audit Process

Audits provide assurance and verification of successful implementation (compliance) based on an evaluation of sufficient and appropriate evidence against defined criteria, such as approved requirements, baselines, and established business practices.[i] The goal of the audit is to provide reasonable assurance to the auditor that the audited entity is operating its part of the BES safely and reliably. Auditing plays an essential role in maintaining confidence that the audited organization is compliant with applicable standardized requirements. NERC CIP audits compliance audits follow a formal methodology outlined in the NERC Compliance Monitoring and Enforcement Program (CMEP) Audit Process (detailed in Appendix 4C of the NERC Rules of Procedure)[ii], guiding the assessment, investigation, evaluation, and auditing of compliance with NERC CIP Reliability Standards.[iii] Ultimately, the CMEP provides the rules by which NERC issues sanctions and ensures mitigation of any confirmed violations. The regulators set the NERC CIP audit schedule. Certain RE types are audited at least once every three (3) years, and others are assessed based on a timetable related to risk and the NERC Compliance Oversight Plan (COP) process.

The Audit Team

The NERC CIP Compliance Audit Team consists typically of the following members from the lead Regional Entity:

Role	Short Description
Audit Team Lead (ATL)	This person is responsible for conducting the audit, acting as the project leader and coordinator, and making the final decision to identify potential non-compliance (PNC) with the reliability standards to be included in the final audit report. The ATL also presents the audit findings to the Registered Entity.
Moderator	This role ensures additional evidence requests are provided, reviewed, clarified, and cataloged, along with communicating preliminary and ongoing findings to stakeholders. In addition, the moderator typically drives the audit by questioning the entity about applicable requirements and clarifying evidence/responses to audit team inquiries.
Scribe	This audit role documents all evidence and composes the draft report.

In addition to these standard audit team members, other members from FERC, NERC, other Regional Entities, and other REs located the same region may participate as observers, based on mutual consent between NERC and the compliance manager for the RE being audited.

Conversely, the RE may object to any member of the compliance audit team on the grounds of a conflict of interest or the existence of other circumstances that could potentially interfere with the team member's impartial performance of their duties. You must provide any such objections in writing to the Compliance Enforcement Authority no later than fifteen (15) days before the start of on-site compliance audit work.

Audit Objectives and Scope

A NERC CIP compliance audit aims to assess the tools, processes, procedures, training programs, internal controls, potential and actual risk, and compliance with the CIP Reliability Standards and Regional Entity CMEP. The audit team will meet these objectives by:

- Reviewing the latest submittals, documentation, and questionnaires
- Reviewing open and recently closed Mitigation Plans
- Assessing compliance with applicable reliability standards
- Providing feedback via an Exit Presentation and Audit Report

The scope of the audit includes:

- A Risk Assessment of the REs functional registrations
- Items covered in the NERC and REs CMEP Implementation Plans
- Possible non-compliance issues from previous audits or self-reports
- Open or closed Mitigation Plans

Audit Types

On-Site Audits

Typically, on-site audits are conducted by the Regional Entity, using a combination of remote documentation review, combined with one or more site visits to the REs home office. The Audit Team Lead (ATL) will also schedule interviews with the REs internal audit team and may ask to schedule interviews with specific personnel from the RE operations, IT, and physical security teams. Additionally, field visits to RE remote facilities may include control centers and substations, as applicable for cyber and physical security inspections. Usually, the audit team performs in-person interviews, so remote subject matter experts (SMEs) may be required to travel to the interview site at the home office.

Virtual Audits

The audit team typically conducts virtual audits with the RE participating remotely via cyber/video connections. Similar to an on-site audit, for Virtual Audits, the Registered Entity will submit documentation in advance of any meetings and may subsequently be required to add details and provide specific evidence demonstrating the desired level of compliance. The ATL usually requests scheduling of online discussions/interviews with the RE audit team members and particular RE personnel, such as those in operations, IT, and physical security. Audit Teams may request that off-site audits also include video-enabled tours.

The 2020-2021 pandemic put physical walk-throughs on hold and required conducting remote facility tours. Virtual audits became the primary, if not the only, type of assessment conducted during that period, creating additional challenges. One of the first challenges with “virtual audit walk-downs” is simply determining which video platform to use. As many Entities and corporations quickly learned during the pandemic, not all videoconferencing platforms are created equal, and maintaining privacy and security presented challenges. No audit participants must use free video-sharing platforms that offer no guarantee of confidentiality. Customers/users of a videoconferencing platform should determine the level of confidentiality provided by the vendor, along with assurances about the security of interactions. Typically, the Regional Entity will not request to record these walk-downs. If a recording is requested, then legal counsel may need to be consulted.

Summary Advice for Remote/Virtual Audits

- Review technology capabilities to ensure appropriate levels of security and confidentiality for sensitive data
- Train team members who will be participating in the audit to effectively and safely use applicable remote platforms
- Test device connectivity along the planned route where you will share live video footage
- Conduct practice runs of web meetings and live-video sharing before the day of the audit
- Appoint an effective Team Lead, and identify and prepare SMEs on the virtual audit process

Notes from the Field

"Getting most people used to the virtual world; that was the main change. That is one thing that this virtual approach has taken away, it's actually the conversations that we have with people. But [the virtual audits have] actually gone really well, because we've been able to have more people available to talk about evidence. Whereas, before, we would have a smaller pool of people able to talk about evidence, now, with a virtual world, it's open to where we don't have to have people travel and can give them an hour to be ready to do an interview at a virtual location. It's actually opened us up quite a bit. Also, for showing audit evidence it's been a little easier because we know it's all going to be virtual, so we have to have the audit evidence ready. "

– Duane Davidson, NERC Regulatory Interaction Manager, Duke Energy

3 Preparing for a CIP Audit

1. Prepare in Advance

It is hard to imagine anyone who believed they had too much audit prep time. With that in mind, develop and maintain an audit preparation schedule thank affords your internal team ample wiggle room. If you identify issues, having such a schedule will provide time to investigate, understand the extent of the inferior condition, and perform in-depth root cause analysis (RCA) where errors appear systemic, develop mitigation solutions, and remediate.

NERC annually posts audit schedules, and REs scheduled for a CIP compliance audit should begin preparations a minimum of six (6) months before the audit date.

Notes from the Field

"Develop the plan now, because this event is just not something that 'happens'. This is a huge event that requires not only time, but requires people not to be stretched - it takes a lot of planning. "
– Duane Davidson, NERC Regulatory Interaction Manager, Duke Energy

"Getting ready for audit is not a last-minute thing. It's not something where you wait for the audit notification to come in. It's really establishing the program from the foundation and maintaining it. The goal is always to be audit-ready. "
- Luis Zaragoza, Regulatory Compliance Manager, BayWa r. e. Solar Projects LLC.

2. Use the Available Tools

There are many resources available to assist with CIP audit preparation. One of the most widely used is NERC's "CIP Evidence Request Tool (ERT)", as discussed in the Audit Timeline and Overview subsection of Section 2: "Audit Process". Start by reading through the ERT user guide that explains the overall tool and reading through the evidence requests themselves. You should definitely be familiar with the ERT and be prepared to respond with the information it requires. Do not create or modify NERC's forms and templates (Yes, we have seen actual cases where some REs have invested much effort in developing their own CIP reporting forms, only to have these rejected by the auditor).

FERC, NERC, and the Regional Entities publish a large amount of helpful information, such as the annual "Staff Report Lessons Learned from the CIP Reliability Audits" as excerpted in Appendix B of this field guide, for quick reference (for links to other valuable sources of information, see Appendix C). By leveraging the knowledge in this report and similar tools, REs can improve their own NERC CIP compliance programs and better prepare for audits (e.g., ITEGRITI has designed an assessment tool, based on the ERT that cross-references key pieces of available NERC information, enabling you to "see" all guidance and organizational knowledge, while gathering and reviewing evidence).

Notes from the Field

"The first step [in preparing for an audit] is not so much the evidence but getting your SMEs in tune with the standard so that they understand what they've been doing and the way we need it to show in evidence. It's actually training the individual to understand their role. You need to have those people trained, and understand their role before we even get into the evidence room. "
– Duane Davidson, NERC Regulatory Interaction Manager, Duke Energy

3. Know your Devices, Firmware, and Software

According to findings from a recent study, the CIP standards with IT-based roots (i.e., CIP-005-6, CIP-007-6, and CIP-010-3) tend to create sizeable challenges for REs.[iv] A fundamental element of any NERC CIP cybersecurity program is a comprehensive inventory of all cyber assets across the enterprise. An RE cannot adequately plan defenses against a coordinated cyberattack without knowing its assets, operating systems, software/firmware, applications, patch levels, and types of information within its area of responsibility (i.e., you cannot secure that which you don't know exists).

CIP-013-1 requires REs to have documented supply chain risk management (SCRM) plans, including verification of suppliers and third parties, integrity and authenticity validation of software, and incident reporting to entities.

The logical next step is determining how those assets should be configured, including a proper CIP-010-3 compliant baseline, and ensuring they stay that way.

Establishing targets for secure settings for both hardware and software allows the organization to adhere to a consistent application of its cybersecurity policy. It also allows unexpected or errant changes to be more quickly and accurately identified, along with comparisons against known baselines. At the same time, effective CIP-010-3 compliant change management practices help mitigate the substantial risks associated with applying inappropriate changes to a production environment, protecting your BCAs, BCSs, and ultimately the BES.

4. Know your Positions

They say the devil is in the proverbial "details", and they are right. Therefore, it comes as no surprise that not everything in the CIP Reliability Standards is binary, and there are many "gotchas". Research has shown that vagueness and prescriptiveness present verbiage challenges. Next to CIP-002-5.1a (categorization), the standards with the interpretation difficulties are CIP-007-6 (patch management and port security) and CIP-010-3 (baselining and change management). CIP-005-6 (electronic access control) and CIP-004-6 (access management) have also been challenging for REs to interpret.[v]

Using previous NERC operating guides as starting points, teams of industry expert volunteers wrote NERC Reliability Standards. The resulting standards can sometimes be "open to interpretation". The first step in understanding CIP Standards requirements is to review the language. Where grey areas exist or where your program relies on multiple compensating controls to achieve the purpose and intent of a requirement, ensure that your team pays attention to small details and has documentation of rationale, approach, and effectiveness. Doing this is essential to NERC CIP audit survival.

Understanding each requirement is vital. Time permitting, we recommend having your RE technical and compliance staff carefully review the individual CIP requirements and note anything they do not understand. Create an outline of significant statements or start a spreadsheet to track your information. This process will also help them prepare other RE personnel involved in an audit.

NERC has a formal process to be invoked when asking for a standard/requirement interpretation if an RE has difficulties determining the verbiage/meaning of a standard requirement. The two key sections in each CIP Standard. The Requirements section describes things the RE needs to do, and the Measures section details evidence the auditors will be checking (although this section is written at a summary level).

5. Pick your Team Wisely

When preparing your RE personnel, having the right team is essential, and leveraging the appropriate skillsets to represent the depth of your compliance program best is critical. To effectively guide these efforts, the importance of a solid internal RE CIP compliance team aligned to the audit cannot be overstated. A strong team leader can keep the audit within the scope and on track (including ensuring that responses are timely) and will be the person all other staff should defer to resolve disputes.

Nothing can derail an audit faster than an internal disagreement in the presence of an auditor. The team lead must also be present during the mock interview phase to help avoid potential surprises during the audit discussions. The team lead must be a seasoned veteran of the audit process, interact effectively with the Regional Entity audit teams, internal RE SMEs, and other personnel.

Notes From the Field

"I would define who's going to lead [the audit] then have a project manager on his or her side, you know, to make sure the plan is well defined and well-orchestrated. The Audit Team Lead is in the virtual interview themselves to understand when the question is not being answered correctly, being answered too much, or going off topic, that's their role. Do not put all the pressure on the SME to know all that. Make sure that everybody understands their role. Got to have gatherers and preparers, and then you've got to have reviewers at the end to make sure that this all tidies up in a nice bow."
– Duane Davidson, NERC Regulatory Interaction Manager, Duke Energy

"Companies sometimes take months and months to hire someone because the required skills and experience is something that is not acquired just anywhere. Even moving between traditional and renewable companies can be challenging because the scope is often very different. You need to find people with good experience who are also flexible, prepared to learn, and eager to take on new challenges to develop their knowledge. [An audit] takes not just the compliance people, but it also takes, for example, field technicians, and engineers. You need to include human resources, for example, when you're dealing with background checks and training. It's going to take a variety of people."
- Luis Zaragoza, Regulatory Compliance Manager, BayWa r.e. Solar Projects LLC.

6. Prepare your SMEs

According to research, organizational priorities, human resources, finance, and budget present significant challenges.[vi] The CIP audit indicates adherence to NERC cybersecurity compliance standards. Auditors will perform thorough risk and gap assessments of what is known, implemented, and documented (KID). However, the RE personnel performing operational, IT, and technical security tasks are likely not compliance specialists.

Help everyone understand that RE reliability, safety, and security are their responsibility, impressing the expectation that they will be respectful and helpful during the audit. SME preparation is paramount to a successful audit, and all your staff need to be helpful, forthcoming, and exceptionally accurate during conversations with auditors.

They don't need to speak through an RE legal representative, but SMEs should address specific questions deliberately, honestly, and concisely. They should be adequately prepared in advance to answer auditor questions and very comfortable with the silence that follows. The appropriate guideline during an audit is that "less is more". One common difficulty REs face is designating the proper people to participate in an audit. Ensuring your internal team includes the appropriate subject matter experts (SMEs) with a strong understanding is imperative.

Your team is critical, so help them organize, plan, and establish effective

preparation metrics. Engage your SMEs early on and often, be methodical, instruct them during one-on-one training, and provide mock audit preparatory sessions. Consider conducting frequent SME briefings and ensure that proposed responses are consistent and clear.

A chatty SME might discuss out-of-scope topics that could potentially influence audit findings (introducing scope creep and bringing something else into range). Role-playing and performing mock audit interviews with your SMEs, using anticipated questions, and gauging the responses.

Conduct a "Mock Audit"

One of the best ways to prepare the SMEs and other RE personnel for an audit is through practice. A "mock audit" will help you to identify potential gaps or shortfalls, along with providing confidence that your SMEs can effectively demonstrate compliance with NERC CIP requirements.

Conducting simulated assessments will help provide assurance that your RE is a thriving organization where everyone knows their job.

During both mock audit practice interviews (and actual audits), it is also a good idea to have at least two SMEs present. Just like everything that is mission-critical in the electric sector, redundancy is essential. You should plan to have backup SMEs lined up "just in case" of unanticipated events. Imagine the potential disruption that could occur if your primary SME is absent on audit day. Treat your SMEs as your "active failover" pair; they are both of equal importance.

Multiple SMEs should also thoroughly review each attachment before sending it to both the mock audit and the actual NERC audit team.

REs typically have trouble performing mock audits due to staffing and timing conflicts or limitations. Therefore, quite a few entities contract with compliance consulting companies to perform readiness assessments just before their audits. Mock audits performed by technically competent third parties also provide a fresh set of proverbial "eyes", helping mitigate the risk of internal bias and identify areas of risk that may have been previously overlooked.

If this option is available to your organization, the third-party assessor should conduct a thorough mock audit, encompassing documentation and evidence reviews, in addition to personnel interviews and facility walk-downs.

7. Ensure Senior Management Involvement

Senior management involvement is crucial to audit success, providing valuable support for preparing and running the audit. In addition to instilling a common goal for personnel, this support can help re-allocate SME time from less significant tasks and allocating appropriate resources and funds. A word of caution is also in order here.

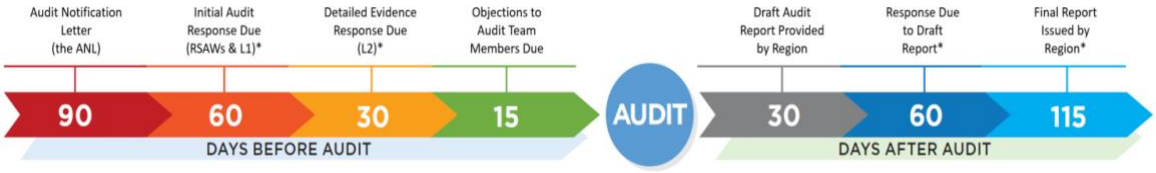
Some well-meaning members of senior management may also require proper coaching to ensure they stick to what is relevant and do not discuss out-of-scope initiatives that could potentially become part of the audit. Similar to SMEs, remember that "less is more" for audits.

4 The CIP Audit Timeline

Audit Timeline and Overview

The timeline of the NERC CIP compliance audit includes the following monitoring times and scheduled dates for audit tasks:

- The monitoring period for newly registered electric entities begins from their registration date.
- The monitoring period for previously audited REs begins on the day after their previous audit exit presentation



NOTE: These timelines and dates are intended as a representative outline and often depend on a prior date to firmly establish them. The Audit Notification Letter (ANL) is sent to the RE at least 90 days before the audit, along with subsequent communications from the Regional Entity, formally establishing the dates and expectations that follow.

90 days before the audit

Ninety (90) days before the audit, the ATL sends the Audit Notification Letter (ANL) to the RE to be audited. This letter typically includes information such as:

- The compliance monitoring period for the audit
- A list of the in-scope audit requirements
- Any initial Requests for Information (RFIs) that must be submitted in advance of the audit, typically:
  - Reliability Standard Audit Worksheet(s) (RSAWs)
  - Level 1 requests/information tabs from the NERC CIP Evidence Request Tool (ERT)**
- Audit Team members
- Non-disclosure information
- Pre-audit materials

***CIP audits almost continually leverage the CIP Evidence Request Tool (ERT), which consists of Level 1, Level 2, and Information Tabs. At a minimum, the Level 1 requests and completed information tabs will typically be part of the initial data request. For more information on the ERT, see the "The CIP Evidence Request Tool (ERT)" subsection of Section 3 "During an Audit" below.*

Note: Evidence can be requested covering the entire three-year audit scope.

60 days before the audit

As directed by the ANL, the RE should typically reply 30 days after receipt of the ANL or up to sixty (60) days before the audit, submitting the following pre-audit materials to the Regional Entity:

- Pre-Audit survev
- General questionnaire
- Review of previous Mitigation Plan documentation
- Completed RSAWs

- Responses to the Level 1 (L1) requests/information tabs from the ERT
    - L1 data requests (DRs), primarily consisting of policies, procedures, and lists of information about the environment
- Additional documentation the Regional Entity requested based on their review of previously submitted documentation

Note: The RE may request a planning conference with the Regional Entity's Audit Team to review audit scope, logistics, and other coordination matters to plan an efficient audit process.

30 days before the audit

The Regional Entity will review the initial submission and reply with Sample Set L2 DRs from the ERT that must also be submitted before the audit. The timeline for these additional submittals will be detailed in the request and vary from region to region. However, this submission of more detailed evidence will typically be expected between fifteen (15) days and thirty (30) before the audit.

15 days before the audit

Although some regions allow for the L2 evidence responses to be submitted later than the 30-day limit, according to the CMEP, the formal deadline for an audited company to object to any of the audit team members from the region usually falls around fifteen (15) days before the audit (sometimes later).

These objections may be raised because of a perceived conflict of interest or other reasons but must be submitted in writing to the Regional Entity before this date.

AUDIT

In practical terms, the audit starts when the Regional Entity receives the initial response submittals from the RE. However, the formal audit period involves some discrete tasks to be performed by the Audit Team, including:

- Preliminary documentation reviews
- Additional documentation requests
- An Opening Presentation
- SME interviews
- Documenting the results & findings
- Exit Briefing

Upon completing the on-site audit tasks, the Regional Entity ATL will present an Exit Briefing to the RE, detailing the process for generating and reviewing the audit draft and final reports.

30 days after the audit

Within thirty (30) business days of the last day of the audit, the Regional Entity will provide the RE with a confidential draft report. The draft report includes the following information:

- A description of the objective, scope, and methodology of the Compliance Audit
- Identification of any evidence of RE potential non-compliance with Reliability Standards, as determined by the Audit Team
- Identification of any Remedial Action Directives, Mitigation Plans or other Mitigating Activities which have been completed or are still pending in the year of the audit
- Identification of any redacted Confidential Information that has been redacted
- Areas of concern and recommendations identified by the Compliance Audit team

60 days after the audit

The RE has thirty (30) business days to respond to the draft audit report. In response to any findings, the RE must develop a corrective action plan to resolve them and provide quarterly status updates of the corrective actions to NERC until they are complete.

115 days after the audit

NERC will issue a final report to the RE forty-five (45) business days after receiving the RE's comments on the draft report. The final report, and the RE's response, will be presented to the NERC Board of Trustees Compliance Committee.

If the audit identifies Possible Violations (PVs), the Regional Entity will issue a Notice of Possible Violation (NoPV) to the RE. The formal enforcement process will then commence as described in the CMEP, including the entity's response to the NoPV, Appeals, Settlement, and Mitigation Plans, as appropriate. NERC will determine any initial penalties and sanctions of serious findings or intentional violations, issuing a Notice of Penalty (NOP) for the RE. The NOP, which becomes effective 31 days after filing, may be appealed by the RE or adjusted by FERC. Rapid application of remedial actions may be required.

NOTE: The Regional Entity, NERC, or FERC do NOT post CIP Audit reports for public consumption due to CIP confidentiality concerns.

5 During a CIP Audit

1. Provide "Quality Evidence"

NERC CIP auditors are trained professionals who know how to assess the evidence. By extension, our goal is to present proof substantiating CIP compliance concisely beyond being secure. Think in terms of "quality evidence" that will pass the "man on the street" test, anticipating and clearly responding to audit questions. This evidence includes three main attributes:

- **Source data** – For each CIP requirement, identify sufficient and appropriate key evidence extracted from a secure source, provide reasonable assurance, and support audit team findings and conclusions. This evidence should be attributable to the system and include appropriate time data to demonstrate when generated (e.g., screenshots showing both date/time and device name).
- **Provide clarity** – Effective quality evidence is focused, containing only the elements requested by the audit team and providing useful "information" instead of just "data". Wherever necessary, embed additional supporting details in the evidence to help clarify and filter out extraneous information that may create confusion. A good practice is adding a section or block (depending on what is supported), summarizing essential points of the evidence presented in narrative format. For example, a concisely worded statement explaining that a signature represents approval and document review has been completed can reduce follow-up questions and annotation efforts.
- **Encompass population** – Ensure the source data is accurate and complete to help ensure all items in the given RE population are effectively captured, addressed, and identified, supporting the audit team's findings and conclusions. Assure evidence accuracy and completeness by comparing different data sets to identify any differences and, when required, take corrective action to resolve deviations.
- **Ensure collaboration** – Avoid "siloed" behavior and utilize cross-functional collaboration within REs, facilitating understanding and evidence consistency. Security is everyone's responsibility, and building solid teams helps increase RE security posture and adds value during an audit.

Preparing the Evidence

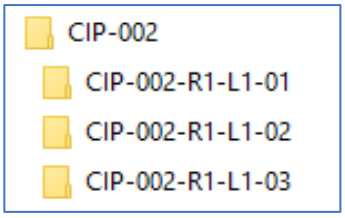
Segregation of duties (SOD) is a fundamental security principle, and gathering the evidence for a NERC CIP audit is a separate discipline from preparing it. Therefore, it is strongly suggested that your "gatherer" not be the same person as your preparer. Additionally, ensuring proper SOD forces a second set of eyes to review the evidence for completeness and accuracy. The RE internal team lead for an upcoming audit is a viable candidate for proper evidence preparation.

Organizing the Evidence

Well-organized and presented evidence greatly assists the audit team, and it can help to expedite the audit. Although research has shown that expectations vary between NERC regions, the goal of the auditors is theoretically to validate RE compliance with the NERC CIP Standards instead of digging down to find areas of non-compliance. You can help facilitate the process by preparing your evidence in a way that promotes your proverbial homework.

Unless a Regional Entity provides different instructions, the audit team will expect the RE to organize evidence by Standard and Request ID (see Figure 1 for sample folder structure) before submitting it to the Regional Entity. Following Regional Entity instructions, methodically organizing the evidence, and referring to exact filenames (including any spaces and dashes within the filename) may enable auditor search tools to identify them and make the audit team's job, plus the overall audit process easier for everyone involved. Remember, the easier you make things for the audit team, the more likely they will help make yours less challenging.

Figure 1 – Sample Evidence Folder Structure



Notes from the Field

"Do not bring anybody in "cold," and do not show any evidence that hasn't been reviewed and already sent to the ERO. "
– Duane Davidson, NERC Regulatory Interaction Manager, Duke Energy

The Critical Cyber Asset List

The RE Critical Cyber Asset (CCA) list is probably the most essential piece of evidence proving compliance with the CIP-002-5.1a standard. The list should be adequately documented and readily available for reference during the audit.

List details should be very clear and consistent regarding the function of every CCA (including BCAs, PCAs, EACMSs, and PACSs) and all its attributes (i.e., name, location, manufacturer, supply chain source, model, serial number, business justification, OS version, firmware version, configuration, interfaces, maintenance, updates/patches installed, commissioning/decommissioning status and other relevant information).

The RSAW

NERC Reliability Standard Audit Worksheets (RSAWs) are crucial written documents for providing evidence of RE documented compliance with specific NERC CIP RSAW requirements. RSAW narratives describe how the RE implements controls in question, and auditors place less emphasis on them than in earlier years. However, they are still valuable for providing the audit team with a foundational understanding of your program and connecting the proverbial "dots" for how things fit together. Therefore, you should prioritize proper RSAW completion.

To help facilitate ongoing compliance and provide a system of "checks and balances," ensure that RSAWs are completed thoroughly and reviewed for accuracy by both RE SMEs and senior management. Third-party consultants performing your mock audit(s) can also help provide RSAW feedback. Beyond being compliant and implementing advanced security controls, the REs goal must concisely present evidence substantiating CIP compliance. The audit team will look for documentation of processes and verification of accurate execution for those actions.

Remember KID? – known, implemented, and documented. During their time at your facility, the audit team will examine all three areas, and the easier you make their lives with robust documentation, the easier they will make yours. Remember, they have lives too.

The CIP Evidence Request Tool (ERT)

The NERC CIP Evidence Request Tool (ERT) spreadsheet-based tool (and related user guide) allows auditors to use pre-defined requests to obtain additional levels of detail not available in the traditional RSAW format.[vii] Similar to an "open book test", these requests proactively provide REs with a better understanding of evidence the audit team requires. The ERT has three (3) main components:

- **Level 1 (L1) Request** – The initial evidence request and consists mainly of policies and procedures. The L1 request is also where lists of specific information about your environment such as BCAs, (e.g., Electronic Security Perimeters (ESPs), Physical Security Perimeters (PSPs), and Transient Cyber Assets (TCAs)) are provided. The audit team will use these lists for the Level 2 request sampling.
- **Sampling** – The audit team then reviews lists provided in response to the Level 1 information request and selects appropriate samples for the Level 2 requests. Sampling sizes should be suitable for the population included in the audit, adhering to the NERC ERO Sampling Handbook guidelines. [viii]
- **Level 2 (L2) Request** – Follow-up data requests (DRs) will ask for more substantive information about specific components of the L1 request. This request may include everything from specific device baselines to detailed authorization records and more. Therefore, you must read the DRs extremely carefully and adequately address the specific audit team's "asks" with quality evidence (as discussed above), demonstrating compliance with related CIP requirements.
- **Additional Data Requests** – The audit team may seek further clarification of L2-provided items (sometimes referred to as Level 3 requests), or they may ask for supplementary information. These requests are often made during the audit interview stages of the audit and are highly variable. Because they depend on L2 requests, they are more challenging to prepare for in advance.

2. Make Your Case

The actual audit period is filled with a large amount of uncertainty because the auditors' questions based on your provided evidence are usually unknown. However, you can help proactively prepare your RE staff by generating a list of anticipated questions and answers during practice sessions and mock audits. An essential component of proper preparation is developing your "compliance story".

During collaborative brainstorming and ideation sessions, your team can help

beyond preparing for RSAW narratives, describing the "culture of compliance and security" surrounding your organizations.

During the audit, you can then share this detailed explanation with the audit team. However, it also affords you a unique opportunity to articulate your "compliance story".

Communications and Conduct

The audited RE should facilitate all communications during the audit, designating a single point of contact (POC) to interact with the audit team. This POC should also encourage the free exchange of information and ideas between the regional audit team members and the RE SMEs. who should be readily available upon request. Back-up SMEs must be accessible and well informed in the event they are needed. Like everything else related to the audit, audit ensuring everything is thoroughly KID is crucial to success.

Interview Conduct and Evidence Presentation

Your RE staff must be prepared to deal with open-ended questions during interviews. However, they may not need to answer them specifically, and it may be enough to ask for clarification. When responding to all auditor questions, answering them succinctly and not straying from the topic is critical. For inquiries outside the bounds of the CIP standards or the audit scope, the RE team lead may intervene, redirecting the question to another team member or asking the audit team for clarification or additional time to respond. Remember that it is possible to showcase the most substantial parts of your CIP compliance and security strategy when providing answers, letting the audit team know that your RE has done its homework.

Because audits can create stressful situations for SMEs and other RE staff, ensure that you instruct them to respond only to "questions" and not to "statements". For each NERC CIP standard, at least one technical or compliance SME with strong familiarity and understanding in their area of expertise must be present to confirm all questions about the audited standard are correctly and thoroughly answered during interviews.

The audit team will test the knowledge of your staff to validate their NERC CIP understanding and application. Therefore, one question may relate to different requirements or standards than the one being audited at that time. It is helpful to predict these interconnections and make sure those additional SMEs are available during the interview process, "just in case".

The RE should also present the evidence during the on-site audit in a meaningful manner that ensures reviewers can understand it, clarifying any vague areas or processes. In summary, be prepared to the best of your ability for any anticipated audit scenarios.

In addition to interviews and assessing the implementation of physical and logical security controls and tools, RE staff training, and internal procedures, the audit team will also conduct a thorough documentation review to determine whether audit program scope requirements are being met. They will evaluate questions related to the completed questionnaires and DRs, along with a random sampling of pertinent evidence.

The audit team may not be familiar with specific acronyms, diagrams, and other procedures your RE uses. When they ask for information, they are usually just trying to get an understanding of your environment. Take your time and explain everything to them since they will help tell your story of compliance. Remember that auditors will be evaluating KID, and in addition to whether CIP requirements are known and implemented, proper and thorough documentation is essential for audit success. During the documentation. review, the audit team will examine policies, procedures, plans, standards, RSAWS, and other documents to determine the effectiveness of the REs compliance program in meeting the CIP requirements.

Notes from the Field

"The biggest thing I always tell folks is, remain calm. Make sure that it's a smooth transaction. We don't want to give any extra opinions or thoughts or ideas. Respond to the question directly, answer that question, and nothing else. One of the challenges is knowing when to speak. Answer the question and let "dead air" be your friend. I know, silence is hard for people, but as long as they're not asking questions, you don't have to answer. "

– Duane Davidson, NERC Regulatory Interaction Manager, Duke Energy

Represent a Culture of Compliance

The RE must demonstrate a robust culture of compliance at every level during the audit process. Ensure copies of governance documentation and policies are readily available and poll multiple levels of your organization for culture "nuggets". Compliance and security are everyone's responsibility, and RE (CIP-004-6) training and awareness programs need to emphasize this.

3. The importance of Logistics

Logistics always plays a vital role in helping the audit to run smoothly. Earlier, we briefly touched on the importance of logistical support. Still, it is crucial to emphasize further some critical areas that might fly below your proverbial "radar" during audit preparation. Before the audit team arrives, you should prepare a private conference room or similar accommodations equipped with network connections, power outlets, video conferencing capabilities, snacks, and beverages to serve as the team's "home base". Additionally, another conference room, large enough to accommodate both the audit team and RE personnel, should be reserved as the main room for audit interviews and meetings. Hosting lunch and dinner daily during the audit is a best practice for building a good climate and spirit of collaboration between the audit team members and your RE staff.

The auditors are your guests during the audit and being a good host and facilitating their comfort is essential for a smooth auditing process. When the audit team arrives at your RE premises, it is advisable to provide them with a tour of the facility, allowing team members can orient themselves.

The RE should appoint a POC to coordinate daily, manage scheduling, and interface with essential RE stakeholders involved with technical and managerial logistics. To avoid scheduling delays, you should pre-arrange the personnel interviews and plan to host a daily senior management and audit team debriefing (a.k.a. "hotwash").

Daily Kickoff

Each morning of the audit, there is usually a daily kickoff meeting. During this meeting, the audit team will summarize the areas and standards they will evaluate that day. The auditors will tell you which SMEs, documentation, and facilities they will require access to, along with asking for any additional supporting evidence. During that time, your RE staff and management will be able to ask questions, gain clarification, or provide helpful feedback. These daily kickoff meetings also provide a forum where your team may add context or present additional proof to assist with your compliance story.

Daily Hotwash

At the end of each day, the audit team will conduct what is known as a daily debriefing (or "hotwash") with the RE team and management. During these sessions, the audit team will summarize their findings based on some preliminary grading scale. All members of your staff must pay close and careful attention. The audit team will usually tell you what they consider compliant and non-compliant based on NERC CIP standard assessment criteria.

Strong collaboration and cooperation are absolutely essential. Be cognizant of the fact that regional audit team members might be sensitive to their authority. In the event of disagreement with the team, patiently and professionally explain your points, tracking and demonstrating to them your culture of compliance across your RE, supplementing with proper historical perspective and context.

It is beneficial to have someone very diplomatic with good negotiation skills on your RE staff participating in the audit. Depending on the rapport the RE has established with the audit team up to that point, the auditors may or may not allow the RE to mitigate specific findings.

The context may depend on the region your auditors represent, along with their background and experience. If you are lucky enough to have an audit team that sees things from a learning and opportunity perspective, they may give you the opportunity for some remediation. On the other hand, if your auditors have more of a "gotcha" mindset, you will face a more significant challenge. Regardless of which group the audit team represents, your goal should still be the same: "all hands on deck" and mitigating/remediating as much risk as possible.

Observations presented by the audit team allow the RE to understand the current perspectives from the auditors, including their assessment methodology and specific areas of focus. Additionally, it helps to identify any misconceptions or confusion that may exist. Preliminary findings fall into two major categories: easily fixed and those requiring more effort to remediate.

That means that when the audit team leaves the premises for the day, it is time for your RE staff to roll up their sleeves and get to work. Address and attempt to mitigate or remediate as many of the hotwash items as possible that evening. Then prepare a written mitigation/remediation report to be delivered to the ATL during the following morning kickoff meeting.

Note: The audit team may or may not agree to accept your overnight mitigation/remediation efforts. Remember that your real goal here is to prove that your RE's actions match what you say, and these efforts demonstrate your culture of compliance to the audit team.

Final Briefing

On the last day of the on-site audit, the audit team will prepare and provide a final report to RE staff and management, summarizing their audit findings. In essence, this is the final "report card" based on the Regional Entity's grading scale. This report will contain a list of results compiled from daily hotwashes, plus discoveries from that final day. The report will include items that do not yet qualify as findings but may require observation and need mitigation or remediation to avoid potential risk. If your RE staff team has been diligent, most or all of these challenges should already have been resolved during after-hours mitigation/remediation work.

The audit team will present the report during a final meeting, which includes your key RE stakeholders. At this point, the findings in the report will have already been recorded by the audit team and submitted to the Regional Entity. Your mitigation/remediation efforts can change nothing more. Actual findings identified by the audit team will be classified

as Potential Non-compliance (PNC) items. Regardless of how you may feel about the list of PNCs and your compliance status, you and your RE team need to politely accept the findings without argument.

The audit team will provide these PNCs to the NERC audit enforcement team. The audit enforcement team then reviews all PNCs, attempts to understand the context surrounding these items, and determines whether they meet NERC for Potential Violations (PVs). After the NERC enforcement team makes its final decisions, the Regional Entity will notify your RE of the outcome and next steps.

Notes from the Field

"You need to make sure that you're way over-prepared in advance, and knowing who's in control, who's going to shut the interview down, who's going to answer the questions, who's going to be the backup to answer the questions, and if this person doesn't know, do we have a person who is online that can speak about this. And [check in with the team] before the interview to make sure that people are still available, because technology happens (somebody is not able to connect, somebody got sick overnight, video [won't work]). You have to have redundancy in all your processes now, because everyone is relying on that internet connection. Everyone. "

– Duane Davidson, NERC Regulatory Interaction Manager, Duke Energy

6 After a CIP Audit

After the audit team leaves, it is vital to capture valuable “lessons learned”, while they are still fresh in the minds of your RE staff. Schedule multiple debriefing sessions where everyone can discuss what they thought went well and areas where things were not smooth and could be improved. Regardless of any issues the Regional Entity audit team may have identified related to your RE’s compliance program, it is essential to take time after the audit to review their findings and observations. Talk about audit team results from daily hotwashes plus the final presentation, making a list of items requiring mitigation action plans (MAPs). Address areas that need improvement, record lessons learned, and securely store all audit-related documentation for reference during the next internal assessment or external audit.

Prepare individual MAPs identifying corresponding weaknesses and areas of non-compliance with specific CIP standards, justifying why these weaknesses exist, and any in-place compensating compliance and security controls that may help mitigate the risk. Use these MAPs to develop corresponding project plans (e.g., Security Incident and Event Monitoring (SIEM) tool enhancements to meet a CIP-007-6 R4 deficiency). Ensure these MAPs and their related project plans are formally approved using your CIP-010-3 change management process, identifying resources required, and estimating milestone and completion dates.

Add the approved MAPs, corresponding project plans, resources required, milestones, and completion dates to your REs Master Plan of Action and Milestones (POA&M). Monitor progress of all MAP items and update Master POA&M line items as they are mitigated/remediated.

Enforcement, Penalties, and Sanctions

NERC relies on the Regional Entities to enforce the NERC Reliability Standards for BES owners, operators, and users based on approved regional delegation agreements. Regional Entities are responsible for monitoring compliance of the registered entities within their regional boundaries, assuring proper mitigation of all violations of approved Reliability Standards, and assessing penalties and sanctions for failing to comply with the NERC CIP standards.

Regional Entity audit team findings will be reviewed using the NERC Compliance Enforcement process and confirmed violations of the mandatory NERC CIP standards might result in sanctions and penalties for the RE under the NERC Sanction Guidelines. These guidelines are primarily based upon violated standards requirements, violation durations, Violation Risk Factors (VRFs), and Violation Severity Levels (VSLs) documented within the NERC CIP standards. Each NERC standard contains VRFs, which determine the risk rating of a non-compliant finding, along with VSLs that assess the degree of non-compliance.

Using VRFs and VSLs, the NERC enforcement team determines applicable sanctions and penalties. NERC may also issue directives to address immediately and deter new or further violations through remedial actions, irrespective of their presence or status (i.e., confirmed or alleged). REs found to violate any standard(s) must submit mitigation plan(s) for approval by NERC. These plan(s) may be created using details from the relevant MAPs and projects in the Master POA&M created earlier. Upon approval by NERC, the RE must execute these plan(s) as submitted. Progress, milestones, and completion status of audit findings may be tracked using the RE’s Master POA&M.

Regional hearing processes are available to resolve contested violations, penalties, or sanctions. If resolution cannot be achieved at the regional level, NERC will listen to escalated disputes through an appeals process. REs or other relevant industry stakeholders can report any perceived inconsistencies in the methods, practices, or tools of two or more Regional Entities using the Consistency Reporting Tool located on the ERO Enterprise Program Alignment Process page of the NERC website.[ix]

7 Beyond the Audit

Organizations invest a great deal of time and energy in interpreting NERC CIP standards and defining the policies, procedures, processes, roles, responsibilities, and technical controls they must implement to help assure compliance. Additionally, they often struggle with ongoing operational, cybersecurity, and CIP compliance responsibilities. Based on recent research, combined with experience, some of the most significant compliance and security challenges faced by utilities include, but are not limited to:[x]

- NERC CIP compliance planning and scheduling
- Human resources and budgeting challenges
- Personnel risk assessment processes for employees and contractors (PRAs) (i.e., CIP-004-6)
- NERC CIP verbiage and interpretation challenges
- Vulnerability to attacks and potentially exploitable weaknesses (e.g., ransomware)
- Proper NERC CIP asset categorization, inventory, and baselining (i.e., CIP-002-5.1a)
- Creation and update of NERC CIP standard policies (i.e., CIP-003-8)
- Creation of formal configuration and change management (i.e., CIP-010-3)
- Achieving compliance with more technical NERC CIP standards (i.e., CIP-005-6, CIP-007-6)
- Supply chain risk management (SCRM) planning and execution (i.e., CIP-013-1)
- Increased NERC focus on going beyond compliance to achieve advanced security
- Ensuring compliance is known, implemented, and fully documented (KID).
- Evidence collection and NERC CIP compliance status tracking
- Thorough identification of all compliance and security gaps
- Robust management, collaboration, and compliance reporting
- Defining and executing timely prioritized remediation plans
- Monitoring of mitigation/remediation status of MAP-related projects in the Master POA&M
- Identifying and self-reporting deficiencies and possible non-compliance
- Performing risk assessments and preparing remediation roadmaps
- Properly preparing and planning for NERC CIP audits
- Effectively and diplomatically negotiating with auditors

How ITEGRITI Can Help

Protecting your IT infrastructure is crucial and recent events demonstrate how a motivated hacker can wreak chaos on well-protected systems.

Recent cyber events, including those impacting the Colonial Pipeline, resulted in increased attention and guidelines from government agencies, including the Department of Homeland Security (DHS), the Transportation Security Administration (TSA), and the Cybersecurity and Infrastructure Security Agency (CISA). Additionally, in the latter part of July 2021, the President signed an Executive Order furthering protection of U.S. critical infrastructure.

ITEGRITI is a cybersecurity consulting and advisory firm with deep expertise gained through our work in protecting large-scale and distributed National Critical Infrastructure since those Standards first became mandatory in 2008. The cybersecurity resilience programs we develop will help you avoid hacks, detect breaches, minimize business disruption during an event, and reduce incident recovery time.

The ITEGRITI leadership team is involved in every project, initially in an advisory capacity during project scoping and organization, followed by direct assignment or oversight roles. Our expertise includes:

- NERC experience since 2006, completed projects in all regions throughout the U.S. and Canada, supporting utilities, transmission, municipalities, cooperatives, and generation representing coal, natural gas, and renewables – wind, solar, hydro and geothermal.
- Management, oversight, or service on over 300 cybersecurity, compliance, and audit projects.
- Industry and consulting backgrounds, combined with IT and OT operational experience.

CIP resources, it can be even harder to find qualified and dependable consultants who can ease the burden from:

- Having more projects or tasks than time or resources to manage
- Ever growing task lists that don't seem to end
- Preparation activities for upcoming audits

ITEGRITI can help in many capacities, including:

- CIP program and compliance assessments
- Facilitate RSAW development
- External, independent, and focused evidence reviews
- CIP mock audits and SME preparation
- vCISO and vComplianceTeam support
    - Risk-based cybersecurity program evaluation
    - Strategic planning, governance, and oversight
    - Technology advisory and steering committee
    - Third-party vendor assessments
    - Process improvement and procedure writing
    - Organizational change management and training
- Dedicated resources to complete projects and task list items
    - Site walkdowns, asset inventory and validation
    - Vulnerability assessments and mitigation management
    - CIP-008 and CIP-009 facilitation and management

ITEGRITI Contacts

Michael Sanchez, CEO
michael.sanchez@itegriti.com
832.781.3177

Dr. Tom Duffey
Director Cybersecurity and Compliance
thomas.duffey@itegriti.com
832.786.1528

itegriti.com

8 Contributors

Lead Authors

Michael Sanchez, ITEGRITI CEO

Sid Shaffer, ITEGRITI Chief Delivery Officer

Dr. Thomas Duffey, ITEGRITI Director of Cybersecurity and Compliance

Advisory Team

Craig Lawrence, NERC CIP SME

Duane Davidson, Duke Energy NERC Regulatory Interaction Manager

Luis Zaragoza, BayWa r.e. Solar Projects Regulatory Compliance Manager

Valued Contributors

Dr. Bill Souza, Executive Cyber Education Chief Executive Officer

Serge Martinez, The Zebra Director of Information Security

Anastasios Arampatzis, BORA

Emma Colburn, BORA

Bob Covello, BORA

Appendix A:

CIP Standards Overview[xiii]

Standard	Short Description	Primary Areas Addressed	Things to Note
CIP-002-5.1a	BES Cyber System Categorization	• Identification and classification of Cyber Assets (High, Medium, assets with Low) • Review of and approval of lists	Inappropriate application of this standard could lead to violations in other applicable standards.
CIP-003-8	Security Management Controls	• CIP Senior Manager identification and approval of cybersecurity policies • Low Impact Asset cyber controls: ○ Cyber Security Awareness ○ Physical Security ○ Electronic Access ○ Incident Response ○ TCA & Removable Media	These are high-level, governance-type requirements.
CIP-004-6	Personnel & Training	• Cybersecurity awareness • Training • Personnel Risk Assessments (PRA) • Access approval and review • Access terminations	Depending on the scope or impact of a change, we recommend that entities consider an organizational change management approach to assist with adoption.
CIP-005-6	Electronic Security Perimeters	• Electronic perimeter configuration ○ Inbound/Outbound access rules ○ Dialup access ○ Malicious communication • Interactive Remote Access	This standard is one of the more technical ones; interpretation and application are essential, and there are areas where many Registered Entities struggle.
CIP-006-6	Physical Security (BES Cyber Systems)	• Physical Access Controls ○ Physical perimeter established and controls established at physical access points ○ Monitoring access to physical access points ○ Logging access to physical access points • Visitor controls • Maintenance and Testing of PACS	Registered Entities should test cyber and physical security convergence to assess the impact of the loss that one has on the other.
CIP-007-6	System Security Management	• Ports and Services • Security Patch Management • Malicious Code Prevention • Logging and Monitoring	Similar to CIP-005-6, this is one of the more technical Standards; interpretation and

		• System Access
		  ○ Shared Accounts
		  ○ Password policies
		  ○ Limited login attempts
			application are the keys. The area where many Registered Entities struggle is in the process/documentation for these asset configurations.

CIP-008-6	Incident Reporting & Response	• Cybersecurity incident response plan
		  ○ Creation
		  ○ Testing
		  ○ Maintenance & updates
		  ○ Notification (E-ISAC, NCCIC, etc.)
			We recommend considering the IR team's needs in determining the intel and assets most beneficial for developing an Emergency Response Plan that accurately evaluates Cyber Security Incidents and documents actions taken and proper notifications made as applicable to each event.

CIP-009-6	Recovery Plans for BES Cyber Systems	• Recovery plan creation
		  ○ Conditions
		  ○ Roles & Responsibilities
		  ○ Backup & Storage
		  ○ Backup verification
		  ○ Data preservation for incidents
		• Recovery plan testing
		  ○ 15-month recovery plan test
		  ○ 15-month information usability test
		  ○ 36-month operational exercise test
		• Recovery plan updates
			In addition to recovery planning, organizations should have quality business continuity processes to minimize business and service disruption until systems are restored.

CIP-010-3	Change Management & Vulnerability Assessments	• Baseline documentation
		• Change authorization
		• Software verification
		• Baseline change monitoring
		• Vulnerability Assessments
		  ○ Every 15 months
		  ○ 36-month *active*
		  ○ Pre-production
		• Transient Cyber Asset (TCA) controls
		• Removable Media controls
			An accurate configuration change management process with the three most important requirements: documentation, documentation, and more documentation are vital to success with this standard.

CIP-011-2	Information Protection	• Identification of BES CSI
		• Protection of BES CSI in:
		  ○ Storage
		  ○ Transit
		  ○ Use
		• Disposal & reuse of devices with BES CSI
			The key to compliance with the requirements of this standard is accurate information identification, classification, protection, and control, including information disposal.

CIP-013-1	Supply chain Risk Management	• The risk assessment process for vendors
		• Procurement process vendor requirements
		  ○ Vendor identified incident notifications
		  ○ Response coordination
		  ○ Vendor access notification
		  ○ Vendor vulnerability disclosure
		  ○ Vendor software verification
		  ○ Coordination of Vendor Interactive Remote Access (IRA)
		• CIP Senior Manager approval
			Well-designed and implemented controls should consider the composition, roles, and responsibilities of the entire IT/OT team, including employees, contractors, vendors, consultants, and regulators.

CIP-014-2[xiv]	Physical Security (Facilities)	• Risk assessment and Physical Security Plans related to:
		  ○ Transmission stations
		  ○ Transmission substations
		  ○ Primary control centers related to above
		• Third-party verification of risk assessments and security plans
			Think guns, guards, and gates related to Transmission stations and substations. Compliance with this standard typically requires a combination of physical security and cybersecurity personnel to develop and implement the systems. One of the potential weak links in this area is the use of contract vendors for physical security and the need for adequate control and documentation of physical security systems.

Appendix B:

FERC Lessons Learned from CIP Audits

Every year, FERC releases the annual "Staff Report Lessons Learned from the CIP Reliability Audits". This report contains valuable information for every Registered Entity to review. The report is careful to point out that while most of the cybersecurity elements adopted by the audited utilities met the minimum requirements of the standards, potential compliance infractions still came to the surface. Additionally, the report includes recommendations that are beyond the scope of the CIP requirements. It is also interesting to note that FERC maps the CIP requirements with NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations and the NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF).

The lessons observed and discussed in the report are intended to help Registered Entities (REs) improve their compliance with the CIP Reliability Standards and their overall cybersecurity posture. The main items and excerpts of the report details for each item are provided here:

1. **Ensure that all BES Cyber Assets (BCAs) are properly identified.**

While entities generally identified (CIP-002-5.1a) BES Cyber Assets (BCAs) effectively, entities did not identify BES Cyber Assets equipment performing supporting functions. Therefore, periodic enterprise-wide network mapping, baselining, and diligent discovery activity are crucial to developing an accurate network diagram to facilitate incident detection, response, and recovery operations.

2. **Ensure that all substation BES Cyber Systems (BCSs) are correctly categorized as high, medium, or low impact.**

While entities generally categorized the impact rating of (CIP-002-5.1a) BES Cyber Systems (BCSs) associated with substations effectively and accurately, in some cases, entities did not adequately consider the interdependency of relay schematics and configurations between control houses containing separate voltage levels.

3. **Ensure that electronic access to BES Cyber System Information (BCSI) is properly authorized and revoked.**

In general, entities appropriately authorized electronic access and access to designated electronic storage locations for BCSI. However, some REs did not consistently apply their documented authorization processes properly or, in cases of termination, did not revoke employee/contractor access to (CIP-011-2) BES Cyber System Information (BCSI).

4. **Consider having a dedicated visitor log at each Physical Security Perimeter (PSP) access point.**

Certain entities share a single visitor log between multiple access points within a single (CIP-006-6) Physical Security Perimeter (PSP), which necessitates moving the log back and forth between access points. Such movements could decrease the security posture for protecting the PSP.

5. Consider locking BES Cyber System (BCS) server racks where possible.

Entities' server racks located in their control centers and substations typically can be locked. Yet not all entities consistently use this capability.

6. Inspect all Physical Security Perimeters (PSPs) periodically to ensure that no unidentified physical access points exist.

In general, entities properly identified all access points to their (CIP-006-6) PSPs. However, some entities did not consider access points, often in the ceilings or other large enough locations for a person to gain access to the PSP, such as maintenance access points.

7. Review security patch management processes periodically and ensure that they are appropriately implemented.

Some entities did not have a consistent (CIP-007-6) security patch management process for applicable Cyber Assets. Staff observed potential risks and areas for improvement in security patch management related to understanding the proper scope of security patch applicability, procedures for tracking applicable security patches, and controls to ensure all relevant security patches are installed or a mitigation plan is in place.

8. Consider consolidating and centralizing password change procedures and documentation.

Entities generally implemented sufficient (CIP-007-6) password change procedures. However, entities that did not use a centralized password database encountered difficulties tracking and monitoring password changes. Entities that primarily relied on databases and spreadsheets to implement password change processes and procedures frequently did not include all applicable Cyber Assets requiring procedural password changes in their accounts. To obtain detail at the appropriate Cyber Asset level, entities relied on multiple sources to track and monitor password change activity. Failure to properly track and document password changes present the risk that accounts may be missed during password changes, which increases the likelihood of compromised passwords.

9. Ensure that backup and recovery procedures are updated promptly.

While entities generally maintained documented processes for the backup and storage of information required to recover BES Cyber System functionality as required in CIP-009-6, R1. 3, some entities failed to update their backup and recovery procedures in a timely manner. For example, in some cases, entities responded to a critical event that required the entity to establish a new process that differed from their documented procedure. In these cases, the entities continued to use the new process without updating their documented process or procedure.

10. Ensure that all remediation plans and steps taken to mitigate vulnerabilities are documented.

Some entities did not report any information to remediate or mitigate vulnerabilities identified in (CIP-010-3) vulnerability assessments, including the planned date of completing the action plan and executing any remediation of mitigation items. Failure to thoroughly document the assessment and subsequent analysis and remediation or mitigation activities could undermine this intent.

11. Ensure that all procedures for tracking the reuse and disposal of substation assets are reviewed and updated regularly.

Some entities could not demonstrate that they adequately disposed of all devices removed from service at substations by following the entities' documented process. In one instance, staff observed that although an entity maintained a strong (CIP-011-2) written information protection program, it failed to document and track some substation devices removed from service. Entities could improve their asset tracking procedures by ensuring that they maintain asset reuse and disposal logs for all substation assets referenced in documented procedures. Failure to properly track the reuse and disposal of substation assets could lead to the improper release or unauthorized retrieval of BCSI contained on the devices.

12. Consider evaluating the security controls implemented by third parties regularly and implement additional controls where needed when using a third party to manage BES Cyber System Information (BCSI).

Entities generally implemented sufficient procedures and controls to protect appropriately and securely handle (CIP-011-2) BCSI, including while in storage, transit, and use. However, some entities relied solely on security controls provided by third-party vendors without first verifying that these controls were sufficient. Failure to ensure the sufficiency of third-party vendor controls could create a risk of compromise to the BCSI if the third-party vendor controls do not provide the necessary level of protection.

Appendix C:

Links to further resources

NERC Glossary of Terms

NERC Standards (with relevant enforcement dates)

Reliability Standard Audit Worksheets (RSAWs)

NERC One-Stop-Shop (Compliance Monitoring & Enforcement Program)

- For the **NERC CIP Evidence Request Tool (ERT),** navigate to "One-Stop-Shop (CMEP, Compliance, and Enforcement) - Active" -> "Compliance" -> "CIP ERT & User Guide"

NERC Compliance Monitoring and Enforcement Manual (CMEP)

2020 FERC staff report details lessons learned from CIP Reliability Audits

NIST Special Publication 800-53r5 – Security and Privacy Controls for Federal Information Systems and Organizations

Blogs

https://itegriti. com/2020/blog/the-ultimate-implementation-guide-for-nerc-cip-008-6/

https://itegriti. com/2020/blog/evidence-request-tool-new-version-4/

https://itegriti. com/2020/blog/nerc-annual-report-2019-overview/

https://itegriti. com/2020/blog/steps-successful_nerc-cip-audit/

Examples of work

https://itegriti. com/2019/cip/efficient-repeatable-cip-validation-process/

https://itegriti. com/2017/cybersecurity/cipv5_cva/

https://itegriti. com/2019/cybersecurity/cipv5-mrre-audit/

https://itegriti. com/2017/cybersecurity/customized-nerc-solutions/

https://itegriti. com/2017/cybersecurity/cip-audit-package-dev-qa/

Endnotes

i As defined by the Information Systems Audit and Control Association (ISACA)

ii https://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx

iii https://www.nerc.com/pa/comp/Pages/CAOneStopShop.aspx [then navigate to "One-Stop-Shop (CMEP, Compliance, and Enforcement) - Active" -> "Compliance" -> "CIP ERT & User Guide"]

iv Exploring the Impact of NERC CIP Regulatory Compliance on Risk and Security for Bulk Electric System Grid Cyber-Attacks: A Qualitative Phenomenological Study - ProQuest H. T. Duffey "Exploring the Impact of NERC CIP Regulatory Compliance on Risk and Security for Bulk Electric System Grid Cyber-Attacks: A Qualitative Phenomenological Study", doctoral dissertation, Northcentral University, December 2018.

v Ibid.

vi Ibid.

vii https://www.nerc.com/pa/comp/Pages/CAOneStopShop.aspx [then navigate to "One-Stop-Shop (CMEP, Compliance, and Enforcement) - Active" -> "Compliance" -> "CIP ERT & User Guide"]

viii https://www.nerc.com/pa/comp/Documents/Sampling_Handbook_Final_05292015.pdf

ix https://www.nerc.com/pa/comp/Pages/EROEnterProAlign.aspx

x Exploring the Impact of NERC CIP Regulatory Compliance on Risk and Security for Bulk Electric System Grid Cyber-Attacks: A Qualitative Phenomenological Study - ProQuest H. T. Duffey "Exploring the Impact of NERC CIP Regulatory Compliance on Risk and Security for Bulk Electric System Grid Cyber-Attacks: A Qualitative Phenomenological Study", doctoral dissertation, Northcentral University, December 2018

xi Ibid.

xii Ibid.

xiii FERC has approved one additional CIP standard (CIP-012-1) that has an upcoming effective date of 7/1/2022. However, because this standard will not be audited until after its enforcement date, it is not covered in this field guide.

xiv CIP-014 is only applicable to Transmission Operator (TOP) and Transmission Owner (TO) registered entities. It should be noted that this standard is often audited separately from the other CIP standards.

DISCLAIMER: This is intended to be a guide, its contents must be reviewed by someone familiar with your unique environment to determine applicability and necessity. Please contact ITEGRITI if you have questions or are looking for advisory, consulting, implementation, or staff augmentation assistance.

INFO@ITEGRITI.COM

ITEGRITI CORPORATE OFFICE

10497 TOWN AND COUNTRY WAY
SUITE 700
HOUSTON, TX 77024

PHONE: +1 832.781.3001

SOUTHEAST REGIONAL OFFICE

101 N TRYON STREET
SUITE 112
CHARLOTTE, NC 28246

PHONE: +1 704.457.9641

FOLLOW US ON LINKEDIN

LINKEDIN.COM/COMPANY/ITEGRITI

JOIN THE NERC CYBER SECURITY PROFESSIONALS GROUP

LINKEDIN.COM/GROUPS/150846

ITEGRITI.COM

INTEGRITY IS OUR CORE VALUE™