SPECIAL TOPICS SERIES · EC-WP-601

Audit Defense Playbook

Practical playbook for entities facing their first NERC audit.

An audit notification letter is not a surprise to a mature program. It is also not the start of preparation, because preparation should already be done. This reference walks a first-time audited entity through what the notice triggers, from the first 72 hours to the exit briefing and the enforcement process that can follow.

Energy Compliance, Inc. Professional Reference

energycomplianceinc.com **OCTOBER 2026**

Disclaimer & Legal Notice

This publication is the work product of Energy Compliance, Inc. and is provided for general information and educational purposes only. It does not constitute legal advice, regulatory guidance, or formal interpretation of any NERC Reliability Standard, FERC order, or Regional Entity directive.

This publication may not be used or cited as authority in any audit, enforcement, regulatory, or legal proceeding. Compliance with NERC Reliability Standards depends on facts and circumstances unique to each registered entity, and the reader should consult qualified counsel and subject matter experts when making compliance decisions.

Statements about NERC procedure in this edition were checked against the NERC Rules of Procedure and its appendices in effect on October 17, 2026. Readers should confirm the current version of any authority cited here before relying on it.

NERC, FERC, and the names of Regional Entities are referenced here for descriptive purposes only. Energy Compliance, Inc. is not affiliated with, sponsored by, or endorsed by the North American Electric Reliability Corporation, the Federal Energy Regulatory Commission, or any NERC Regional Entity.

Energy Compliance, Inc. assumes no responsibility or liability for errors, omissions, or outcomes resulting from the use of this publication.

Foreword

This professional reference is one of a series Energy Compliance, Inc. publishes for registered entities and the people who run their compliance programs.

I've spent more than thirty years on every side of the bulk electric system. I've operated control centers as a Reliability Coordinator, Transmission Operator, and Power System Operator. I've audited grid facilities and signed off on findings as a senior compliance auditor. I've worked enforcement matters from inside the regulator's process. For the last several years I've advised registered entities directly through the firm I founded.

The entities that do reliability well share a common habit. They take the standards seriously without confusing them with reliability itself. They know that a NERC Reliability Standard is a floor, not a ceiling. They know that compliance is something an auditor evaluates, but reliability is something a system either delivers or doesn't. They prepare for audits by building programs that survive real questions, not binders that look thick.

That's the perspective these references try to share. Each one focuses on a single topic: a standard family, an operational function, a regulatory framework, or an emerging industry challenge. Each one walks through how the topic actually works.

These references are written for the compliance manager who wants to understand the system, not just memorize requirements. For the legal counsel who has to brief a board honestly. For the senior operator who's been told that compliance and reliability are the

same thing and suspects they aren't. And for the new compliance hire who got handed a binder and told good luck.

These references aren't marketing material disguised as content. They come out of three decades of doing this work and watching it succeed and fail. I've written them in the same voice I use in a control room or in front of a Regional Entity audit team: direct, grounded in evidence, and honest about what the standards do and do not require.

Energy Compliance exists because most of the consulting offered to registered entities today is structured for billable hours rather than for outcomes. A senior practitioner oversees every engagement. We don't bring five people to a meeting that needs one. We automate the work that should be automated, and we apply senior judgment to the work that requires it. If that approach matches what you're looking for in a compliance partner, the back of this reference has our contact information.

Executive Summary

An audit notification letter is not a surprise to a mature program. It is also not the start of preparation; preparation should already be done. What the notice triggers is execution, on a timeline the auditor sets and under procedural rules the program either knows or doesn't. First-time audited entities lose audits in predictable ways, and the patterns are well known to anyone who has sat on an audit team. Knowing them in advance is the most efficient form of preparation.

- Without a defined command structure, audit response fragments. The auditors notice, and findings follow.
- An internal pre-audit is the cheapest way to find issues. Once the notification letter arrives, self-report credit for in-scope requirements is generally gone, so the pre-audit has to happen first.
- Auditors interview people. The interviews surface what the documentation conceals.
- RFI overproduction is a trap. Sending more than the RFI requested gives auditors more material in which to find issues.
- The most common first-time failure is a program documented one way for the auditors and operated another way in practice. The auditor finds the gap.
- The audit close isn't the end of the matter. The draft audit report, the comment period, and any enforcement action that follows can run for months.

1 You Got the Letter, Now What

The audit notification letter is not a surprise in the operational sense. Under the NERC Compliance Monitoring and Enforcement Program (CMEP), the Compliance Enforcement Authority, which for most entities is the Regional Entity, must tell a registered entity at least 270 days ahead that it plans an audit, then send the formal notice at least 90 days before the audit begins (Appendix 4C, Section 4.1.1). What the letter does is convert a future obligation into an immediate one. The response in the first 48 to 72 hours sets the trajectory for everything that follows.

Read the Notification Carefully

The 90-day notice identifies the Reliability Standards to be evaluated, names the audit team members and their recent employment history, sets the beginning and end dates of the audit period, and requests documents, data, and information by a Required Date (Appendix 4C, Sections 4.1.1 and 4.1.3.2). Every one of these details matters. The list of standards defines which requirements are in play and what the auditors are there to examine. The audit period defines how far back your evidence has to reach. The Required Date determines how much preparation time is available before the first evidence submission is due. The team roster matters too: an entity that sees a conflict of interest has to object in writing no later than 30 days before the audit starts (Appendix 4C, Section 4.1.4.4).

First-time entities frequently make the mistake of treating the notification as a general alarm rather than a specific document. They mobilize broadly before understanding precisely what has been requested. The result is effort spent gathering evidence for requirements that are not in scope, and evidence gaps in the requirements that are. Read the letter. Build the response around what it actually says.

Establish Command and Control Immediately

Audit defense is a coordination problem. It requires pulling evidence from multiple organizational functions, briefing personnel who interact with auditors, managing RFI response timelines, and keeping one consistent account across all of those activities at once. Without a defined command structure (a single person or a small core team with clear authority and accountability), coordination breaks down within days.

The audit lead does not need to be the most technically knowledgeable person on the compliance team. They need to be the person who can hold the process together: tracking what has been submitted, what is pending, who is responsible for what, and where the timeline is at risk. In organizations that lack this role, audit responses fragment. Evidence goes in inconsistently, different people answer RFIs with different approaches, and personnel briefings produce contradictory accounts of the same controls.

Do Not Submit Evidence You Have Not Reviewed

The first evidence submission in a CIP audit establishes the baseline from which auditors conduct their examination. The Regional Entities use a common CIP Evidence Request Tool for this. Its Level 1 requests ask for asset, cyber asset, and personnel populations along with programs and procedures; the audit team then draws samples from those populations and issues Level 2 requests for detailed implementation evidence on the sampled items (CIP Evidence Request Tool User Guide, January 2026). Whatever you submit at Level 1 becomes the population the auditors sample from. Evidence in the initial package that contains inconsistencies, errors, or gaps will generate RFIs immediately, and those RFIs tell the audit team the program was not thoroughly reviewed before submission.

Every document in the initial submission should be reviewed by someone who understands both what the document says and what the requirement expects it to demonstrate. This is not a review for accuracy in the abstract. It is a review of whether the document actually addresses the requirement it is meant to satisfy, and whether it agrees with the other documents in the package that address related requirements.

End-of-Chapter Summary

The audit notification triggers a coordination challenge that first-time entities underestimate. The first 72 hours should produce a clear audit response structure, a precise understanding of scope, and a review process for evidence before submission. Entities that skip these steps spend the rest of the audit recovering from the gaps they created at the start.

> **From the Field**
>
> The audit notice is not a surprise to a mature program. It is also not the start of preparation; it is the start of execution. Preparation should already be done.
>
> Without a defined command structure (one accountable person, a small core team, clear authority), audit response fragments. The auditors notice. Findings increase.
>
> Day one of the audit is not the day to assemble the team. The team is the program. The audit is when the program performs.

2 Building Your Audit War Room

Audit defense requires a temporary operational structure that does not exist in most compliance organizations under normal conditions. Calling it a war room is not hyperbole. Audit response is high-tempo, deadline-driven coordination, and it needs dedicated resources, clear roles, and a physical or virtual space where the work is centralized.

Who Must Be in the Room

The core audit team needs four functional capabilities: someone who understands the CIP requirements deeply enough to evaluate whether evidence satisfies them; someone who can access and produce technical evidence from the systems being audited; someone who manages the administrative workflow of submissions, deadlines, and RFI responses; and someone with the organizational authority to resolve disputes and make decisions when they arise.

In smaller entities, one person may cover multiple functions. In larger entities, each function may require a team. What cannot be allowed is for any of these functions to go unrepresented, particularly the technical evidence function. Compliance teams that cannot independently access system logs, configuration records, and access management data depend on technical staff who may not understand the evidentiary requirements. The result is evidence that is accurate but not responsive.

Mapping Evidence to Requirements Before Auditors Ask

Before the first auditor interaction, the audit team should have a complete map: every in-scope requirement, every piece of evidence that addresses it, where that evidence is located, who produced it, and what period it covers. This map is the audit team's internal reference. It lets the team respond to RFIs quickly, find gaps before auditors do, and keep every evidence submission consistent with the last.

Entities that build this map during audit preparation frequently discover requirements for which they have evidence, but the evidence does not actually demonstrate what the requirement demands. Better to discover that during internal review than in the middle of an RFI cycle, when the clock is running and the auditors are watching response quality closely.

Centralize Everything

Evidence in an audit must be traceable and consistent. When different team members pull documents from different locations, with different naming conventions and different version control, the evidence package becomes internally inconsistent. The same system appears under different names in different documents, the same date appears in different formats, and the same access review shows up in different versions. These inconsistencies do not

necessarily indicate control failures. They do tell auditors the evidence was assembled rather than maintained, and that invites a closer look at the underlying controls.

Centralizing evidence before the audit begins, whether in a shared drive, a compliance management platform, or a structured folder hierarchy, is not bureaucratic overhead. It is the control that makes the rest of the audit response work.

End-of-Chapter Summary

The audit war room is a temporary operational structure with four required functional capabilities and a centralized evidence repository. Entities that build this structure before they need it produce more coherent audit responses than entities that improvise it under pressure, and the time spent setting it up is repaid many times over once RFIs start arriving.

> **From the Field**
>
> Audit response is high-tempo coordination. It needs dedicated resources, clear roles, and a centralized space where the work happens.
>
> The war room isn't theatrical. It's operational. It's the place where evidence is staged, RFI responses are drafted, and the audit timeline is tracked.
>
> A war room set up after the audit notice is a war room running behind. Mature programs keep a virtual war-room template they can activate within a day.

3 Control Validation: Find Your Issues Before Auditors Do

Audit preparation is not just evidence assembly. It is a control verification exercise: an internal audit conducted before the external one. The goal is to find gaps, inconsistencies, and documentation failures while there is still time to address them, and to go into the audit with an honest understanding of where the program is strong and where it has exposure.

Timing matters for a second reason. Under the NERC Sanction Guidelines, receiving a notification letter that lists the requirements in scope generally ends the entity's eligibility for self-reporting credit on those requirements until the engagement is over (Appendix 4B, Section 3.3, note 8). A gap found and self-reported before the letter arrives can earn mitigating credit. The same gap found after the letter usually cannot.

The Internal Gap Assessment

For each in-scope requirement, the audit team should ask two questions. Does the control the requirement demands actually exist in the operational environment? And does the evidence demonstrate that it exists? These are different questions with potentially different answers. A control can exist without adequate documentation. Documentation can exist without the underlying control. In our experience, the first situation is a documentation problem that is far easier to resolve. The second is a control failure, and that is where real enforcement exposure sits.

The internal gap assessment should be performed by people who understand both the requirement and the operational environment. A compliance analyst who knows the standard but has never seen the control center cannot assess whether the access control process described in the policy is actually implemented in the system. A systems administrator who knows the technical environment but has never read the CIP requirements cannot assess whether the operational practice meets the standard's evidence expectations. Effective gap assessment requires both.

The Evidence Quality Test

Evidence quality has a specific meaning in the CIP audit context. Quality evidence demonstrates three things: that the control exists, that it was implemented during the period under examination, and that it was implemented consistently throughout the audit period, not just on the day the auditor visits. Appendix 4C is explicit on the last point. The entity's data and information must show compliance for the entire period covered by the audit (Section 4.1.3.2).

First-time entities frequently produce evidence that demonstrates current compliance without demonstrating historical compliance. A current access review roster shows that accounts were

reviewed recently. It does not show that they were reviewed on the required schedule throughout the audit period. A current network diagram shows the ESP boundary today. It does not show where the boundary sat six months ago, a date the auditor's sample may well include. Evidence that addresses only the present state, when the requirement calls for consistent implementation over time, creates findings rather than resolving them.

Where a standard sets a retention period shorter than the audit period, Appendix 4C says the entity will not be found in noncompliance solely for lacking records it was entitled to discard, but it will still be required to demonstrate compliance through other means (Section 4.1.3.2).

Prioritize By Risk, Not By Requirement Number

Audit preparation time is finite and the requirements in scope are numerous. Entities that spread preparation effort evenly across all requirements will spend as much time on low-risk, well-documented controls as on high-risk, underdocumented ones. That is the wrong allocation.

Prioritize control validation by the combination of control complexity, evidence maturity, and enforcement consequence. Requirements where the control is operationally complex, the evidence has not been tested, and a finding would carry significant penalty exposure deserve the most preparation attention. Requirements where the control is straightforward, the evidence has been routinely maintained, and the consequence of a finding is modest can be reviewed more efficiently.

End-of-Chapter Summary

Control validation before the audit is an internal verification exercise. It needs people who understand both the requirement and the operation, it should produce an honest assessment of where the program has exposure, and it should allocate effort by risk rather than by requirement sequence. Entities that conduct genuine pre-audit validation go into the audit already knowing what the auditors will find.

> **From the Field**
>
> An internal pre-audit is the cheapest way to find issues. What you find yourself, you can fix and self-report on your own schedule. What the auditors find, you answer for on theirs.
>
> Honest pre-audit means identifying gaps, not building cases for them. The goal isn't to defend the program against the pre-audit; it's to learn from it.
>
> The pre-audit takes weeks. The audit takes weeks. Programs that compress the pre-audit shortchange the very preparation they need to defend the audit.

4 SME Preparation: The Human Element of Audit Defense

Of all the elements of audit defense, subject matter expert preparation is the one most often neglected and the one that most directly shapes audit outcomes. Auditors interview people. Those interviews surface what documentation conceals and show whether the operational environment reflects the compliance program on paper.

What Auditors Are Actually Looking For in Interviews

An auditor conducting a subject matter expert interview is not administering a test of regulatory knowledge. The auditor is assessing whether the person understands how the controls they are responsible for actually work in daily operations, as opposed to how the policy document describes them. The SME who can explain a control in operational terms, describe what would happen if it failed, and identify who else in the organization is involved in carrying it out is demonstrating a level of control ownership that documentation cannot convey.

The SME who recites policy language, defers to the compliance team on interpretation, or cannot describe what "medium impact" means for their specific operational environment (the BES Cyber System categories come from CIP-002-5.1a) is demonstrating the absence of control ownership. Auditors read that as a warning sign, however complete the documentation is.

Preparing SMEs Without Over-Scripting Them

SME preparation walks a difficult line. Auditors can recognize scripted interview responses: multiple people using identical language to describe the same control, answers that are suspiciously polished for operational personnel, or a narrative that breaks down under follow-up questions the script did not anticipate. Over-scripted SMEs present almost as poorly as unprepared ones, because the scripting signals that the compliance team does not trust its SMEs to represent the program accurately.

Effective SME preparation focuses on three things. The SME understands the control they are responsible for in operational terms. The SME understands the boundary of what they should and should not address in an interview. And the SME knows how to handle a question they cannot answer, which is not "I don't know" but "Let me get you the documentation on that" or "That question is better directed to our engineering team," naming whichever group actually owns the answer.

Consistency Is More Important Than Completeness

When multiple SMEs are interviewed about related controls (the network engineer about ESP architecture, the security analyst about access management, the operations supervisor about

change management), their accounts must be consistent. Not identical, but consistent: describing the same process, referencing the same systems, characterizing the same organizational structure.

Inconsistency across SME interviews is one of the most reliable indicators to auditors that the compliance program exists on paper but not in operation. If the network engineer describes the ESP as including System A and the security analyst describes it as excluding System A, the discrepancy is not a question of whose memory is better. It is evidence that the ESP boundary is not clearly understood or consistently applied, and that goes to the heart of CIP-005-7 Requirement R1, Part 1.1, which requires every applicable Cyber Asset connected to a network via a routable protocol to reside within a defined ESP.

FERC approved CIP-005-8 and ten other modified CIP standards in Order No. 919 (March 19, 2026), revising the ESP and related definitions to accommodate virtualization. NERC lists CIP-005-8 as subject to future enforcement on July 1, 2028, with CIP-005-7 retiring the day before. The implementation plan FERC approved also lets an entity adopt the new standards early, at six, 12, or 18 months after the order's May 26, 2026 effective date, by notifying its Regional Entity. Know which version governs your audit period before the first evidence submission. A consistent, well-understood boundary will matter just as much under the new version.

End-of-Chapter Summary

SME preparation is the audit defense activity with the highest return on investment. Auditors interview people to surface what documentation conceals. SMEs who own their controls operationally, who can explain them, describe their failure modes, and discuss their organizational dependencies, give the auditors something documentation alone cannot. SMEs who recite policy language or defer to compliance on operational questions confirm the auditors' concern that documented and operational compliance have drifted apart.

> **From the Field**
>
> Auditors interview people. The interviews surface what the documentation conceals.
>
> An SME who knows the documentation but not the operational reality is a vulnerability. An SME who knows the operational reality but not the documentation is also a vulnerability. The mature program has SMEs who know both, and it rehearses them.
>
> The interview prep that gets skipped is the prep that produces findings. An afternoon of SME rehearsal costs far less than mitigating a finding afterward.

5 Managing RFIs: Speed, Accuracy, and Discipline

Requests for Information are the main instrument auditors use to probe the compliance program between formal audit activities. The quality of RFI responses (their accuracy, their responsiveness to what was actually asked, and the timeliness with which they are produced) is a direct signal to auditors about the maturity of the program and the entity's capacity to operate under regulatory scrutiny.

Treat every response as a formal record. Appendix 4C requires any submission of information the CMEP calls for to be signed by an officer, employee, attorney, or other authorized representative of the entity (Section 4.0).

The Overproduction Trap

The instinct of many first-time audit teams is to answer every RFI with as much documentation as possible, on the theory that more evidence is better evidence. In practice it is not. Responses that bury the responsive evidence in irrelevant material signal two things to auditors: that the compliance team does not clearly understand what was asked, and that the program generates documentation faster than it generates control. Neither signal is favorable.

Respond to what was asked. Produce the evidence that addresses the specific request. If additional context is needed to make the responsive evidence intelligible, include it with a clear explanation of its purpose. Do not pad RFI responses. Auditors read everything submitted in response to an RFI, and they notice when the volume of material is out of proportion to the question.

The Underproduction Trap

The opposite failure, providing less than what was asked, is more consequential than overproduction. An RFI response that does not address every element of the request generates a follow-up RFI, extends the audit timeline, and suggests either that the evidence does not exist or that the audit team is managing disclosures. Neither is the impression a first-time entity wants to create.

Before submitting any RFI response, the audit lead should verify that every element of the request has been addressed, that the responsive evidence covers the full period specified in the request, and that the response is consistent with evidence previously submitted. RFI responses that contradict earlier submissions require explanation, and explaining contradictions is almost always harder than preventing them.

The Timeline Is a Test

RFI response deadlines are not suggestions, and the CMEP has a formal escalation path for missed ones. If requested documents, data, or information do not arrive by the Required Date, the Regional Entity may send a notice giving the entity five business days to produce the material or propose a date. If that notice goes unanswered, a second notice, copied to the chief executive, gives ten business days. After that, the Regional Entity may issue a Notice of Alleged Violation at the Severe Violation Severity Level for the requirement in question (Appendix 4C, Attachment 1). Even short of that path, a missed deadline, or an extension request without a compelling operational reason, suggests either disorganization or deliberate delay. Either impression damages the audit posture.

The audit war room should track every outstanding RFI, its deadline, and the current status of the response. When a deadline is at risk, escalate the issue to the audit lead early enough to either accelerate the response or request an extension before the deadline passes. Attachment 1 itself allows the Regional Entity to grant reasonable additional time when the entity asks before the Required Date and explains the basis in reasonable detail. A proactive extension request with an explanation of the operational reason is received very differently than a missed deadline followed by a late submission.

End-of-Chapter Summary

RFI management is audit defense in its most visible form. The accuracy, completeness, and timeliness of responses tell auditors as much about the compliance program as the evidence itself. First-time entities that treat RFI response as an administrative chore rather than a strategic one consistently produce responses that raise more questions than they resolve.

> **From the Field**
>
> RFIs are how auditors ask the questions that find findings. Every response is a signed submission that becomes part of the audit record.
>
> Overproduction is a trap. Sending more than the RFI requested gives auditors more material in which to find issues. Send what's asked, and only what's asked.
>
> RFI cadence signals program maturity. Late, scattered, or contradictory responses signal a program operating under pressure. Disciplined responses signal a program that knows itself.

6 Common First-Time Audit Failures and How to Avoid Them

Across years of audit experience on both sides of the table, the failure patterns in first-time CIP audits are consistent. They are not random. They reflect predictable gaps between how compliance programs are designed to operate and how they actually function under external scrutiny. Knowing these patterns in advance is the most efficient form of audit preparation.

Failure One: The Evidence That Proves Too Much

One of the most common first-time audit failures is submitting evidence that, on careful examination, reveals a compliance gap the entity did not recognize. An access review spreadsheet meant to demonstrate periodic review may show, on closer reading, that certain accounts were left out of the review, or that the reviewer lacked the authority to approve access at the required level. An audit trail log submitted to demonstrate security event monitoring may contain events that, under the applicable requirements, should have triggered an investigation that cannot be evidenced.

This failure mode, evidence that creates findings rather than resolving them, comes from submitting documents without reading them from an auditor's perspective. The pre-submission review in Chapter 1 and the evidence quality test in Chapter 3 are designed to catch it before anything goes out.

Failure Two: The Corrective Action That Looks Reactive

When auditors identify a potential finding, entities sometimes respond by rapidly implementing the missing control and producing evidence of implementation. The corrective action is real. But if it was implemented after the audit began, the evidence of implementation also reveals the period during which the control was absent, and that is the exposure period for the finding.

Fix the gap anyway. Appendix 4C requires noncompliance to be mitigated (Section 4.0), and a Mitigation Plan is not an admission of a violation (Section 6.1). The failure is presenting a mid-audit fix as if the control had always been in place. A control implemented during the audit does not erase the period before it; only a remediation effort that was documented and under way before the audit began shows good-faith compliance for that earlier period. Be candid about the timeline and let the mitigation speak for itself.

Failure Three: The Scope Concession

Auditors occasionally pursue lines of inquiry that go beyond the scope stated in the notification, examining systems, time periods, or requirements the letter did not list. First-time entities, unfamiliar with how audit scope is set, sometimes respond to these inquiries as though they were in scope and produce evidence for requirements not formally in play.

This is not an adversarial dynamic. The Regional Entity tailors audit scope through its risk-based processes and may include any Reliability Standard applicable to the entity (Appendix 4C, Section 4.1.3.1), and any potential noncompliance it learns of, by whatever means, goes to a Preliminary Screen (Section 4.8). Auditors may legitimately follow evidence where it leads. But entities are entitled to understand the basis for any inquiry that appears to exceed the stated scope, and an entity that believes a request for documents or information is unreasonable may ask the NERC general counsel for a written determination (Section 4.0). An experienced compliance lead or external advisor recognizes when a scope question is worth raising and how to raise it constructively.

Failure Four: Losing Organizational Composure

Audits create institutional stress. Personnel who are not accustomed to external scrutiny may become defensive, evasive, or inconsistent under audit pressure. Leadership may intervene in ways that disrupt the audit response structure. Communication that should flow through the audit lead starts flowing around it. The coherent audit posture built in preparation fractures under the pressure of the real event.

The antidote is structural. An audit response structure with clear roles, clear communication protocols, and a single point of coordination holds up under pressure better than one that depends on individual composure. When the structure is clear, the organization knows how to function even when the people in it are stressed.

End-of-Chapter Summary

First-time audit failures are not random. They reflect predictable gaps between how programs are designed and how they perform under external scrutiny. Evidence that creates findings, reactive control implementation, scope management failures, and breakdowns in organizational composure are the four most common patterns. Each can be anticipated and addressed before the audit begins, which is the only time addressing them is fully effective.

> **From the Field**
>
> First-time audits fail in predictable ways. The patterns repeat from audit to audit. Knowing them in advance is the most efficient form of preparation.
>
> The most common first-time failure is a program documented one way for the auditors and operated another way in practice. The auditor finds the gap.

7 Closing the Audit and What Comes Next

The formal close of a NERC CIP audit is not the end of the process. It marks the move from evidence review to audit reporting and, where potential noncompliance was identified, to enforcement. How an entity manages that transition shapes outcomes that persist long after the audit itself.

The Preliminary Findings Discussion

Appendix 4C requires the audit team to conduct an exit briefing with the entity (Section 4.1.1). This is where the audit team shares its initial observations: potential noncompliance, inconsistencies, or concerns that emerged from the evidence review and interviews. It is not the formal determination, which comes later. It is the entity's first opportunity to understand what the audit team has identified and to provide context that may affect how those observations are characterized.

The exit briefing is a technical and factual conversation. The entity's response should focus on accurate context: explaining operational conditions, clarifying evidence that may have been misread, and pointing to supplementary documentation that addresses the auditor's concern. It is not the place for argument, denial, or legal positioning. Those conversations come later, in writing, if an observation turns into an enforcement matter.

Responding to Formal Findings

The written record starts with the audit report. The audit team prepares a draft report identifying any evidence of potential noncompliance, and the entity has 30 days to comment on it and to identify Confidential Information proposed for redaction before the report is finalized (Appendix 4C, Section 4.1.5). Use that window. Factual corrections are far easier to make in the draft than after the report goes to NERC.

Potential noncompliance in the final report then moves through the enforcement process. The Regional Entity screens and assesses it and may resolve it as a Compliance Exception or through Find, Fix, Track and Report, or it may pursue it as an Alleged Violation by offering settlement or issuing a Notice of Alleged Violation and Proposed Penalty or Sanction (Appendix 4C, Sections 4A, 5.1 and 5.3). The entity then has 30 days to accept, contest the penalty, or contest both the violation and the penalty; silence counts as acceptance (Section 5.3). An entity that contests must file a signed written response within that 30 days, and the Regional Entity must schedule a conference within ten business days of receiving it (Section 5.4). Settlement can be requested at any time (Section 5.6).

That written response is one of the most consequential documents an entity will produce in the enforcement process. It establishes the factual record, characterizes the nature and scope of the issue, presents mitigating factors, and describes corrective actions. The Sanction Guidelines name several of the factors that matter, including the presence and quality of the entity's internal compliance program, the degree and quality of its cooperation, and self-reporting with voluntary mitigation (Appendix 4B, Section 3.3).

A well-drafted response demonstrates that the entity understands the requirement and the nature of the gap; that the gap was corrected promptly once identified; that the corrective actions address root cause, not just the immediate error; and that the compliance program has systemic controls designed to prevent recurrence. A poorly drafted response minimizes the finding without addressing it, disputes it on technical grounds the evidence does not support, or offers corrective actions that are obviously inadequate. That kind of response damages the entity's credibility, and in my experience it leads to worse outcomes.

What Comes After: Building on the Audit Experience

The first audit, whatever its outcome, is the most valuable compliance program assessment an entity will ever receive. It shows, with precision and authority, where the program is strong and where it is not. Entities that treat the audit outcome, even a difficult one with multiple findings, as actionable intelligence rather than a verdict to be survived consistently improve their programs between audit cycles.

The post-audit corrective action plan should address not just the specific findings but the process and governance gaps that produced them. Appendix 4C already requires a Mitigation Plan to identify the cause of the noncompliance and the activities that will prevent recurrence (Section 6.2). Go further than that minimum. Let the audit experience inform the next revision of the compliance program's structure, its documentation requirements, its evidence maintenance practices, its SME preparation, and its cadence of internal assessments. The entity that comes out of its first audit with an accurate picture of its program and a plan aimed at root causes is in a far better position than one that treats the audit as a closed event and moves on.

End-of-Chapter Summary

Closing the audit well takes technical precision at the exit briefing, care in the comment period and any enforcement response, and the organizational discipline to turn audit results into real program improvement. The entities that use their first audit as a program assessment tool, rather than an obstacle to be cleared, build compliance programs that perform better in every audit cycle that follows.

Glossary of Terms

Term	Meaning in this paper
Audit Notification	The formal notice a Regional Entity sends at least 90 days before a scheduled Compliance Audit. It identifies the Reliability Standards to be evaluated, the audit team members and their recent employment history, the audit period, and the documents, data, and information requested (Appendix 4C, Sections 4.1.1 and 4.1.3.2). A notice of the planned audit comes at least 270 days ahead.
Compliance Monitoring and Enforcement Program (CMEP)	The NERC program in Appendix 4C to the Rules of Procedure, or a Regional Entity's FERC-approved program, through which compliance with Reliability Standards is monitored and enforced. Compliance Audits are one of its monitoring processes.
Evidence	Documentation demonstrating that a required control exists, was implemented during the relevant period, and was implemented consistently. The entity's evidence must show compliance for the entire audit period. In our experience, auditors give the most weight to records produced when the control was performed rather than reconstructed afterward.
Exit Briefing	The meeting at the close of a Compliance Audit at which the audit team reviews its observations with the entity, required by Appendix 4C, Section 4.1.1. This paper also calls it the preliminary findings discussion.
Finding	Informal shorthand for potential noncompliance identified by an audit. A Compliance Audit report identifies evidence of potential noncompliance; whether a violation occurred, and any penalty under the NERC Sanction Guidelines, is decided through the enforcement process in Appendix 4C, Section 5.
Mitigation Plan	An action plan developed by the registered entity to correct a noncompliance with a Reliability Standard and prevent its recurrence (Rules of Procedure, Appendix 2). Appendix 4C, Section 6.2 requires it to address the cause of the noncompliance and recurrence, and submitting one is not an admission of a violation.
Notice of Alleged Violation and Proposed Penalty or Sanction (NAVAPS)	The notice a Compliance Enforcement Authority (NERC or a Regional Entity) issues when it determines that evidence indicates a violation and Compliance Exception or FFT treatment is not appropriate. It starts a 30-day period for the entity to accept or contest (Appendix 4C, Section 5.3).
Notice of Penalty (NOP)	The notice NERC prepares and files with FERC stating the penalty or sanction for a Confirmed Violation or settlement (Rules of Procedure, Appendix 2). NERC publicly posts each NOP for violations of non-CIP standards, with the violator's identity, when it files with FERC (Appendix 4C, Section 8.0).
Preliminary Findings Discussion	See Exit Briefing.

Term	Meaning in this paper
Regional Entity (RE)	An entity with enforcement authority under 18 C.F.R. § 39.8 (Rules of Procedure, Appendix 2), operating under a delegation agreement with NERC. Acting as the Compliance Enforcement Authority, a Regional Entity conducts Compliance Audits of the registered entities in its area, including CIP audits.
Request for Information (RFI)	A written request from the audit team for specific documentation, data, or information during a Compliance Audit. Responses become part of the audit record and must be signed by an authorized representative of the entity (Appendix 4C, Section 4.0).
Reliability Standard Audit Worksheet (RSAW)	The worksheet NERC publishes for a Reliability Standard describing what auditors evaluate and the evidence they expect for each requirement. RSAWs exist for CIP and non-CIP standards and are posted on NERC's website.
Subject Matter Expert (SME)	The person responsible for explaining a specific control or operational practice to auditors during interviews. SME preparation and interview consistency are among the most consequential factors in audit outcomes.

How Energy Compliance Can Help

Everything in this playbook is work I have done from both chairs. If your first audit notice is on the calendar, or you suspect it will be soon, these are the three places where our team earns its keep.

Audit preparation and defense. We run the internal pre-audit described in Chapter 3 the way the Regional Entity will run the real one: in-scope requirements mapped to evidence, evidence read for what it actually proves, SMEs rehearsed without a script, and the RFI desk staffed from the Required Date through the exit briefing. Where potential noncompliance surfaces, we draft the draft-report comments, the NAVAPS response and the Mitigation Plan so they hold up in Section 5 of Appendix 4C, not just in the meeting.

RSAW narrative development and monthly evidence. Most first-time findings trace to evidence that was assembled for the audit instead of maintained for it. We write the RSAW narratives against the enforceable standard version and set up the monthly evidence production so the audit package already exists when the letter arrives.

Data Request management. When the RFIs start, we map every request to a deliverable, deduplicate against what has already been submitted, tighten scope to what was actually asked, and sequence the responses so nothing contradicts an earlier submission.

WattOps Compliance. WattOps Compliance is EC's NERC compliance evidence platform, at wattopscompliance.com. If you want to see what maintained evidence looks like before you commit to anything, we will run one standard at one of your facilities through WattOps at no cost. CIP standards are excluded from that offer.

RenewOps. RenewOps is EC's renewable operations monitoring and analytics platform, with a Data Center module. For a solar, wind or storage fleet, audit evidence that depends on operations data (alarms, availability, event logs) holds up best when that data is captured and kept the same way every day, and that is what RenewOps is for.

If you have a notice in hand, send it to me and I will tell you what the first 72 hours should look like for your program.

Website: energycomplianceinc.com · Email: rsmith@complianceforenergy.com · Phone: 763.438.4427

About the Author

Rob Smith is the Founder and Principal of Energy Compliance, Inc., with more than thirty years in the industry on every side of the system. He began in control-room operations as a Reliability Coordinator, Transmission Operator, and Power System Operator across RTO/ISO and utility control centers. On the regulator side, he was a senior compliance auditor and subject matter expert for NERC Reliability Standards. He audited grid facilities, evaluated mitigation adequacy, participated in risk-based oversight of utility mitigation activities, and supported the development of violation notifications and settlements in FERC-directed enforcement actions. He conducted a regulatory audit in the Sultanate of Oman against the Sultanate's Sector Law and Grid Code.

He founded Energy Compliance, Inc. to deliver senior regulator-side compliance authority without the layered staffing and billable-hour overhead of larger firms.

Education:

- MBA, Energy Management, University of Mary
- MSL, Compliance Law, Fordham Law University
- BAS, Energy Management, Bismarck State College
- BAS, Mechanical Engineering, Metallurgy minor, University of Florida
- BAS, Criminology, St. Petersburg College (State Law Enforcement Certification)
- AAS, Power Plant Technology, Bismarck State College
- AAS, Electrical Transmission System Technology, Bismarck State College

Certifications: NERC Lead Auditor training; previously NERC-certified at the Reliability Coordinator level; 1st Class A Boiler Engineer License, Minnesota.

The views expressed in this publication do not represent the views of NERC, FERC, or any Regional Entity.

About Energy Compliance, Inc.

Energy Compliance, Inc. is an independent consulting and advisory firm focused exclusively on electric reliability, cybersecurity reliability, and regulatory compliance for organizations connected to the North American Bulk Electric System.

Our work supports registered entities, including Generator Owners and Operators, Transmission Owners and Operators, Reliability Coordinators, Balancing Authorities, and Distribution Providers. We work across NERC Reliability Standards, FERC orders, RTO/ISO market participation rules, Regional Entity oversight, and state regulatory frameworks.

We do this work differently than larger consulting firms. A senior practitioner with regulator-side experience oversees every engagement, and our team is sized to the work. We staff for outcomes, not for billable hours. Our deliverables are written to be operationally executable and audit-defensible, not to manufacture activity. Where automation can replace manual work, we build the automation. Where senior judgment is required, the senior is in the room.

Audit defense services include:

- Pre-audit gap assessment and evidence quality review
- Mock audit facilitation with experienced auditor perspective
- SME preparation and interview coaching
- RFI response strategy and document review
- Exit briefing and draft audit report response preparation
- Formal enforcement response and mitigation plan development

Energy Compliance services more broadly include, but are not limited to:

- NERC reliability and compliance advisory support

- Reliability governance and program assessments
- Registration and applicability analysis
- Operational and engineering reliability alignment
- Compliance program design and improvement
- Audit and enforcement support (non-advocacy)
- Mitigation planning and Self-Report development
- Training and executive briefings on reliability frameworks
- Regulator-perspective program reviews

Each engagement is scoped to the entity's role, function, and bulk system impact. Every engagement is grounded in direct audit experience, not theoretical compliance guidance, and Energy Compliance operates with complete independence from regulatory and oversight bodies.

Energy Compliance is not affiliated with, sponsored by, or endorsed by the North American Electric Reliability Corporation, the Federal Energy Regulatory Commission, or any Regional Entity.

Website: energycomplianceinc.com · Email: rsmith@complianceforenergy.com · Phone: 763.438.4427

Sources and Authorities

NERC Rules of Procedure

- NERC, Rules of Procedure, Rules of Procedure in Effect table (accessed October 17, 2026). https://www.nerc.com/who-we-are/rules-of-procedure
- NERC, Rules of Procedure (without appendices), effective November 28, 2023, including Section 400 (Compliance Enforcement) and Section 1200 (Regional Delegation Agreements). https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/nerc-rop.pdf
- NERC, Rules of Procedure Appendix 2, Definitions Used in the Rules of Procedure, effective June 27, 2024 (definitions of Compliance Audit, Compliance Enforcement Authority, CMEP, Alleged Violation, Mitigation Plan, Notice of Penalty, Regional Entity). https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-2.pdf
- NERC, Rules of Procedure Appendix 4B, Sanction Guidelines of the North American Electric Reliability Corporation, effective January 19, 2021, Section 3.3 (aggravating and mitigating factors) and note 8 (effect of a notification letter on self-reporting credit). https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-4b.pdf
- NERC, Rules of Procedure Appendix 4C, Compliance Monitoring and Enforcement Program, effective May 19, 2022, Sections 4.0, 4.1.1, 4.1.3, 4.1.4.4, 4.1.5, 4.8, 4A, 5.1 through 5.6, 6.1, 6.2, 8.0, and Attachment 1 (Process for Non-submittal of Requested Data). https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-4c.pdf

NERC Reliability Standards and audit tools

- NERC, Reliability Standard CIP-005-7, Cyber Security, Electronic Security Perimeter(s), Requirement R1, Part 1.1; mandatory and enforceable since October 1, 2022. https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-005-7.pdf
- NERC, Reliability Standard CIP-005-8, standard page showing status "Subject to Future Enforcement" with effective date July 1, 2028 (accessed October 17, 2026). https://www.nerc.com/standards/reliability-standards/cip/cip-005-8
- NERC, Reliability Standard CIP-005-7, standard page showing status "Mandatory Subject to Enforcement," effective October 1, 2022, inactive date June 30, 2028 (accessed October 17, 2026). https://www.nerc.com/standards/reliability-standards/cip/cip-005-7

- NERC, Reliability Standard CIP-002-5.1a, Cyber Security, BES Cyber System Categorization, Attachment 1 impact rating criteria. https://www.nerc.com/standards/reliability-standards/cip/cip-002-5.1a
- NERC, Reliability Standard Audit Worksheets (RSAWs). https://www.nerc.com/programs/compliance/reliability-standard-audit-worksheets-rsaws
- NERC, Critical Infrastructure Protection Evidence Request Tool User Guide (January 2026), posted on the NERC CMEP Resources page February 5, 2026. https://www.nerc.com/globalassets/programs/compliance/cmep-resources/cip-evidence-request-tool-user-guide-v10.pdf
- NERC, CMEP Resources page, listing CIP Evidence Request Tool v10.1 (posted September 24, 2026) and the User Guide v10 (accessed October 17, 2026). https://www.nerc.com/programs/compliance/cmep-resources

Federal Energy Regulatory Commission

- Virtualization Reliability Standards, Order No. 919, Docket No. RM24-8-000 (issued March 19, 2026), 91 Fed. Reg. 13957 (March 24, 2026), effective May 26, 2026. https://www.govinfo.gov/content/pkg/FR-2026-03-24/html/2026-05716.htm

© Energy Compliance, Inc. · EC-WP-601 · Status as of October 17, 2026