FOUNDATIONS SERIES · EC-WP-105

Why Entities Fail Audits

The patterns behind NERC audit failures and how to build a program that doesn't repeat them

Audits don't fail randomly. The failure patterns are public. Knowing them in advance is most of the work.

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, engineering advice, or formal interpretation of any NERC Reliability Standard, FERC order, RTO or ISO protocol, or state commission rule.

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.

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're the result 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, evidence-grounded, and honest about what the standards do and do not require.

Energy Compliance exists because much of the consulting offered to registered entities today is structured for billable hours rather than for outcomes. Every engagement is overseen by a senior practitioner. We don't bring five people to a meeting that needs one. We automate the work that should be automated. 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.

If not, the reference still belongs to you. Take what's useful. Apply it well. And remember the only test that ultimately matters: when the system needs to perform, does it?

Rob Smith

Founder and Principal, Energy Compliance, Inc.

Executive Summary

Audits don't fail randomly. The patterns are public. NERC posts its non-CIP Notices of Penalty when it files them with FERC, and its annual CMEP report names the standards that draw the most noncompliance and the root causes behind them. Read enough of that record and the same failure modes show up over and over. Documentation that doesn't match operations. SMEs who can't speak the standard out loud. Self-Reports that should have been filed two years earlier. Scope assumptions made once and never revisited. Knowing these patterns in advance is most of the work of preparation. Entities that operate as if the audit could happen tomorrow rarely fail the audit that actually arrives.

- Audits don't fail because the standards are unclear. They fail because programs operate differently than they document.
- The most common audit failure isn't a missing control. It's documentation that doesn't reconcile with what operators actually do. NERC's 2025 annual report points the same way: across the dispositions coded to date, deficient policies and procedures lead for CIP and ineffective preventive controls lead for everything else.
- An SME who can't explain the program in their own words is a finding waiting for an interview.
- Self-Report timing changes the enforcement posture. The Sanction Guidelines credit a prompt Self-Report, typically within three months of discovery, and an audit notification letter generally ends that credit for the requirements in scope. A late Self-Report is a finding with extra steps.
- Scope drift kills programs slowly. Unmanaged change becomes audit findings for every month it went unnoticed.
- Noncompliance clusters around a short list of standards. In 2025, CIP-010, CIP-007 and CIP-004 led the CIP list, and PRC-005, MOD-025 and FAC-008 led the operations and planning list. The pattern is reproducible, and so is the prevention.
- The strongest audit-defense posture isn't having no findings. It's having no surprises.

The rules cited here come from the NERC Rules of Procedure and their appendices, CIP-002-5.1a, FERC's regulations and NERC's 2025 annual report. Where a statement is my judgment rather than a rule, the text says so.

1 The Real Reason Audits Fail (Hint: It's Not What You Think)

Most analyses of audit failure focus on control gaps. The actual failure mode is usually the gap between what the program documents and what operators do.

1.1 The Controls Usually Exist

Across decades of audit experience on both sides of the table, the failure patterns in NERC audits cluster around the same handful of root causes. Programs fail audits because they document one thing and operate another. They fail because SMEs can't reconstruct the reasoning behind decisions made years earlier. They fail because evidence packages were assembled for the binder, not for the question the auditor will actually ask.

The control-gap explanation gets too much attention. In my view, the controls existed in most failed audits. Someone designed and implemented them. The auditor found the gap between the control design and the operational reality, or between that reality and the documentation meant to describe it.

1.2 The Pattern Is on the Public Record

The same root causes show up in Self-Reports, in Notices of Alleged Violation and Proposed Penalty or Sanction, and in settlement agreements. Under Appendix 4C, NERC posts each non-CIP Notice of Penalty when it files it with FERC.

NERC's 2025 annual report says the same across the nearly 2,800 dispositions coded to date. Deficient policy and procedures is the leading root cause for CIP issues, and ineffective preventive controls for everything else. Neither is an unclear requirement, although the report does list lack of understanding among the leading causes for MOD-025. Both describe a program that doesn't do what it says.

1.3 The Most Expensive Failure Mode

Programs that internalize the pattern early build different programs from those that wait for the audit to teach them. What you avoid by understanding it is the program that looks audit-ready on paper, conducts well during the kickoff meeting, and then comes apart during the SME interviews. In my view that is the most expensive failure mode, because the program looked successful right up until it wasn't.

> **From the Field**
>
> Most failed audits don't have a missing control. They have a control that doesn't match its description.

2 The Documentation-vs-Operation Gap

Documentation that drifts from operations is, in my view, the most common audit failure mechanism. The drift is slow, predictable, and preventable.

2.1 How Documentation Drifts

Documentation drifts the moment it stops being maintained as a living artifact. A procedure written three years ago describes the operation as it existed three years ago. Since then equipment was replaced, software updated, personnel rotated and scope adjusted, and the documentation didn't keep up.

Procedure updates are work. They get scheduled, and then they get deferred. Six months becomes twelve becomes twenty-four, and the procedure on the shelf turns ceremonial. Operations runs on tribal knowledge and recent practice, not on the procedure. The auditor reads the procedure, watches the operation, asks why they don't match, and writes a finding.

2.2 The Audit Period Covers All of It

Drift matters more than most programs assume because of how the audit period works. Under Appendix 4C, Section 4.1.3.2, the entity's data and information must show compliance for the entire period the audit covers. That period begins the day after the End Date of the prior Compliance Audit. For an entity never audited before, it begins on the later of June 18, 2007 or the date the entity became subject to the standards.

So a procedure that was wrong for eighteen months of a three-year audit period is not a current-state problem. It is eighteen months of exposure. One protection exists: where a standard's retention period does not cover the whole audit period, the entity will not be found in noncompliance solely for lacking information it rightfully did not retain. The CEA will still require it to demonstrate compliance through other means.

2.3 Keep Documentation Inside the Operation

Programs that survive audits keep documentation current as part of the operation, not adjacent to it. Every operational change triggers a documentation review. Every quarter, someone compares the documentation to actual practice. Every annual cycle, the procedures get walked through with the SMEs who execute them. None of this is exotic. It's discipline, and many programs eventually let it lapse.

2.4 One Finding or a Programmatic One

The cost of the lapse compounds. A single procedure out of date is a finding. A pattern of out-of-date procedures across the program reads as a programmatic failure, and the Sanction

Guidelines treat that differently. Appendix 4B lists programmatic failures involving the same or similar requirements among the repetitive infractions that can aggravate a penalty. It also notes that an entity with a poor-quality or failed compliance program may have violations of increased risk, and that NERC or the Regional Entity may increase the sanction on that basis. The auditor doesn't have to find every gap. They only have to find enough to establish the pattern.

> **From the Field**
>
> My rule of thumb: a procedure nobody has reviewed in 18 months is wrong, even if you haven't noticed yet.

3 Evidence That Tells Two Stories

Evidence packages are supposed to demonstrate compliance. Many demonstrate something different, and the auditor reads both.

3.1 One Story or Two

Evidence is the backbone of audit defense. It's also where many programs reveal more than they intended. A well-built evidence package tells one consistent story: the program operated as designed, the controls executed as required, and the documentation reflects both. A poorly built package tells two stories, what the program was supposed to do and what it actually did.

3.2 Where Evidence Breaks

The common failures are ordinary ones: timestamps that don't reconcile across sources, log entries that show controls executing in ways the procedures don't describe, screenshots from systems that have since been decommissioned, evidence dated three years ago when the procedure says the review is quarterly. All of them cost findings.

3.3 Build Evidence as a Live Deliverable

Evidence that holds up is built as a live deliverable, not compiled after the fact. Each control execution should leave its own evidence behind, and each artifact gets cataloged with its provenance. When the auditor asks for samples, the program produces them quickly because they were maintained, not assembled.

The audit tells you what it will ask: NERC posts its Reliability Standard Audit Worksheets (RSAWs) on its website. Build the evidence against the RSAW before the audit notice, not after. Someone also has to vouch for it. Appendix 4C requires any report or other submission the CMEP requires to be signed by an officer, employee, attorney or other authorized representative of the entity.

3.4 Inconsistency Expands the Audit

Two-story evidence has another consequence: it draws scrutiny. In my view, an auditor who finds one inconsistency starts looking for more. The conversation shifts from procedural to investigative. Requests for information multiply and the interview scope widens. The program that thought it had a simple audit ends up with a complex one, because the evidence raised questions the auditor felt obligated to chase.

> **From the Field**
>
> Evidence that doesn't reconcile tells the auditor more than the program intended.

4 The SME Who Couldn't Speak the Standard

SME interviews surface gaps that documentation conceals. Programs that don't prepare their SMEs end up with findings the documentation alone wouldn't have produced.

4.1 Where the Documentation Stops Protecting You

The SME interview is one of the most consequential phases of any NERC audit. The auditor reads the documentation and reviews the evidence. Then the auditor talks to the people who actually do the work, and that conversation surfaces gaps documentation can't conceal. Programs that prepare SMEs get through this phase. Programs that don't take findings they otherwise would have avoided.

4.2 The SME Who Can Recite but Not Explain

In my view, the most common SME failure is an SME who can't explain, in their own words, why the program is structured the way it is. They can recite the procedure. They can describe the control. What they can't do is explain the rationale, the context or the operating reality behind it. To the auditor, that signals a program whose documentation was written by one set of people and executed by another, with no shared understanding of why.

4.3 The SME Who Contradicts the Procedure

The second common failure is an SME who contradicts the documentation, or contradicts themselves across questions. It usually isn't intentional. The SME knows the operation better than the documentation, and when the questions are framed against the documentation, they answer from operational memory. The answer is right operationally and wrong against the documented procedure. The auditor records the discrepancy.

4.4 Rehearse Before the Auditor Arrives

Preparation matters, and it is finite. In my view, a few hours of focused SME rehearsal cost far less than the mitigation that follows a finding. Mature programs run dry-run interviews internally, with someone playing the auditor, well before the real audit arrives. The rehearsal should test rationale as well as recall: why the control exists, what it protects, and what the evidence would show if the auditor asked for it today.

> **From the Field**
>
> When the SME contradicts the documentation, the auditor doesn't decide who's right. The auditor records both versions. Rehearsal hours are cheap. Mitigation hours are not.

5 Scope Drift and Why You Didn't Notice

Compliance scope changes when operations change. Programs that don't track scope continuously end up with audit findings on systems they didn't realize were in scope.

5.1 Scope Is the Foundation

Scope is the foundation of every NERC compliance program. It determines which standards apply, which assets are relevant, which controls are required, and which evidence has to be maintained. Scope decisions made at registration get embedded in the program design. Scope decisions never re-examined become audit findings.

5.2 How Scope Moves, and Who Notices

Operations change continuously. Assets get added, removed, repurposed and reclassified. Appendix 5A to the Rules of Procedure requires a registered entity to submit changes in its registration information to its Regional Entity. On the CIP side, CIP-002-5.1a rates BES Cyber Systems as high, medium or low impact against its Attachment 1 criteria, and a change at the asset can move a system from low to medium. Scope assumptions that were correct three years ago can be wrong today, and the program built on them has gaps it doesn't know about.

The auditor will catch the drift. The asset inventory gets compared against operational reality. The categorization gets re-validated against current function. The systems that should be in scope but aren't get identified, and they bring with them every requirement that should have applied during the period they were misclassified.

5.3 Review Scope Continuously

On scope, the practice that holds up is continuous review. A scope reassessment follows any operational change, and the scope inventory is reconciled against the operating environment each quarter. The annual scope review is documented, evidenced and cross-checked.

For CIP, part of the cadence is mandatory. CIP-002-5.1a Requirement R2 requires a review of the R1 identifications, and CIP Senior Manager or delegate approval, at least once every 15 calendar months. None of this stops scope from drifting. It stops the drift from going unnoticed.

> **From the Field**
>
> The auditor reconstructs scope from operational reality, not from your stated scope. The two had better match.

6 Self-Identification: The Posture That Changes Everything

Self-Reports are not admissions of failure. They are the most strategic tool in audit posture management.

6.1 The Decision That Frames the Rest

The decision to Self-Report is one of the most consequential decisions in any compliance program. A timely Self-Report changes the enforcement posture, can narrow the penalty exposure, and frames the regulator's view of the program. A late Self-Report, or a violation the auditor finds first, does the opposite. Appendix 4C encourages Self-Reports at the time an entity becomes aware that it has, or may have, violated a Reliability Standard.

A Self-Report must include a risk assessment of the noncompliance, a description of its extent, its cause, and the actions taken or planned to mitigate it, including preventing recurrence. That covers the cause and correction content a Mitigation Plan also needs under Section 6.2.

6.2 What the Sanction Guidelines Reward

The Sanction Guidelines in Appendix 4B make self-reporting a mitigating factor. NERC or the Regional Entity considers whether the entity self-reported within a reasonably prompt time after becoming aware of the violation, and before detection through a compliance monitoring engagement or a notification of an upcoming one. An entity should submit a Self-Report as soon as practical, but typically within three months of discovery.

The timing rule has a hard edge. Receipt of a notification letter for an upcoming Compliance Audit, Spot Check or Self-Certification that details the requirements in scope generally terminates self-reporting credit for those requirements until the engagement is over. If you suspect a problem in a requirement that may be in next year's scope, report it before the 90-day audit notice arrives.

6.3 What the ERO Reads Into Self-Reports

NERC says plainly how it reads self-reporting. Its 2025 annual report states that the ERO Enterprise looks for high levels of self-reported noncompliance as an indicator of good detective controls and strong cultures of compliance. It reports that about 85 percent of reported noncompliance was self-identified, both in 2025 and over the last five years.

That base rate shapes the audit conversation. In my view, an auditor who sees no Self-Reports from a large program is looking at either an unusually clean program or an unusually opaque one, and will work out which. Programs that under-report eventually surface their issues at

audit, and the conversation turns to why the issue never came through a Self-Report. The answer decides whether the discussion is about the violation or about the program's culture.

6.4 Make It Routine

Mature programs Self-Report routinely, even on minor matters. They build the discipline, normalize the conversation with the Region, and show continuous self-assessment. By the time the audit arrives, the Region already has a record of the program's candor, and that record shapes the audit posture.

> **From the Field**
>
> The decision not to Self-Report a known issue is the decision to let the regulator frame it.

7 Audit Findings as Diagnostics

An audit finding is information. The right response treats it as a diagnostic, not just a problem to mitigate.

7.1 Mitigation Is the Minimum

Most programs treat audit findings reactively. The finding arrives, the Mitigation Plan gets drafted, the corrective action gets implemented, and the matter closes. That is the minimum response. It satisfies the regulator. It doesn't make the next audit better.

Even the minimum asks more than many programs give. Appendix 2 defines a Mitigation Plan as an action plan to correct a noncompliance and prevent its re-occurrence. A plan that fixes the instance and leaves the cause meets half of that.

7.2 Read the Finding for Cause

Mature programs treat findings as diagnostics. Each finding signals something about the program: a process gap, documentation drift, a training shortfall, a coordination failure. The mitigation addresses the immediate finding. The diagnostic addresses the systemic issue that produced it. In my view, programs that do both see their finding rates fall over time, and programs that do only the first see the same findings audit after audit.

Reading findings this way takes honesty. The temptation is to treat each finding as isolated, the fault of one person or one moment and therefore not a sign of anything broader. That framing avoids hard internal conversations and produces no improvement. The programs that improve are the ones willing to ask whether the program design itself enabled the finding.

7.3 Repeat Findings Change the Math

Findings also age. A finding from three years ago that produced no programmatic change will likely produce a similar finding three years from now, and the Region notices repeat patterns. The Sanction Guidelines make repetitive violations and compliance history an aggravating factor. Repetitive infractions that may aggravate a penalty generally include prior violations still ongoing within five years of the start of the current one that either share its root cause with mitigation that should have prevented recurrence, or are programmatic failures involving the same or similar requirements.

The ceiling is not trivial. As adjusted for inflation in 18 C.F.R. § 385.1602(d), the maximum civil penalty under the Federal Power Act is $1,584,648 per violation, per day.

> **From the Field**
>
> The mitigation closes the finding. The diagnostic prevents the next one.

8 Building the Audit-Resistant Program

Audit resistance isn't a posture you adopt during preparation. It's a program design choice made early and reinforced continuously.

8.1 Small Disciplines, Maintained

The audit-resistant program isn't built during audit preparation. It's built years earlier, through deliberate design choices that compound. The choices aren't dramatic. They are small disciplines maintained over time: documentation kept current, evidence captured continuously, SMEs trained on rationale and not just procedure, scope reviewed quarterly, Self-Reports filed routinely, findings analyzed for cause.

8.2 Preparation That Looks Like Operations

The hallmark of an audit-resistant program is that audit preparation looks no different from normal operations. The documentation is already current. The evidence is already organized. The SMEs already know how to talk about their work, and the scope is already verified. When the 90-day notice arrives, the program answers from what it already keeps. The audit is a checkpoint, not a sprint.

8.3 The Region as a Peer

Programs that reach this state share another trait: they treat the Region as a peer, not an adversary. The Regional Entity's role is to monitor and enforce compliance with the Reliability Standards, as the Compliance Enforcement Authority for its area. The program's role is to deliver reliability and demonstrate compliance. Both sides benefit from clean, transparent, ongoing communication. In my view, programs that maintain that relationship have different audits from programs that keep their distance.

8.4 The Return on Discipline

The investment is real, and so is the return. In my view, audit-resistant programs spend less on emergency mitigation, legal defense and reputational repair, and they absorb less of the operational disruption that comes with an extended enforcement matter. The discipline is the price.

> **From the Field**
>
> The strongest audit posture isn't having no findings. It's having no surprises, for the entity or for the regulator.

Glossary

Term	Meaning in this paper
Audit period	Under Appendix 4C, Section 4.1.3.2, the period for which an entity must show compliance in a Compliance Audit, beginning the day after the End Date of the prior audit.
BES Cyber System	As used here, the unit CIP-002-5.1a rates high, medium or low impact.
Compliance Audit	Under the NERC Rules of Procedure, a systematic, objective review and examination of records and activities to determine whether a Registered Entity meets the Requirements of applicable Reliability Standards.
Compliance Enforcement Authority (CEA)	NERC or the Regional Entity, in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.
Compliance Monitoring and Enforcement Program (CMEP)	The NERC program set out in Appendix 4C to the NERC Rules of Procedure, or a Regional Entity's Commission-approved program.
Mitigation Plan	An action plan developed by the Registered Entity to correct a noncompliance with a Reliability Standard and prevent re-occurrence of the violation.
Notice of Alleged Violation and Proposed Penalty or Sanction (NAVAPS)	A notice issued by the Compliance Enforcement Authority to a Registered Entity under Section 5.3 of Appendix 4C.
Notice of Penalty	A notice prepared by NERC and filed with FERC, following NERC approval of a notice of Confirmed Violation or a settlement agreement, stating the penalty or sanction imposed or agreed to.
Registered Entity	An owner, operator, or user of the Bulk Power System, or the entity registered as its designee for compliance purposes, that is included in the NERC Compliance Registry.
Regional Entity	An entity having enforcement authority under 18 C.F.R. § 39.8.
Reliability Standard Audit Worksheet (RSAW)	An audit worksheet NERC posts on its website under Appendix 4C, Section 4.1.
Scope drift	As used here, the gap that opens when assets or categorizations change and stated scope does not.
Self-Report	A report by a Registered Entity stating that it believes it has, or may have, violated a Reliability Standard.

How Energy Compliance Can Help

Every pattern in this reference is cheaper to find before the auditor does. Here is where we help.

Audit preparation and audit defense

EC provides NERC compliance program support, interpretation and audit preparation; audit and enforcement support (non-advocacy); and audit defense, including Notice of Penalty response and settlement posture. RSAW production and data request strategy build the evidence against the question the auditor will ask, and SME preparation is part of the work.

Self-Reports, mitigation and program reviews

EC provides mitigation planning and Self-Report development. Regulator-perspective program reviews and reliability governance and program assessments test whether documentation, evidence and scope still match operations. Compliance program design and improvement, and ongoing compliance program management, close the gaps they find.

Advisory, registration and engagement

EC also provides NERC reliability and compliance advisory support, senior advisory with direct engagement on complex reliability questions, registration and applicability analysis, operational and engineering reliability alignment, training and executive briefings on reliability frameworks, and industry engagement in standards development and working-group participation. Each engagement is scoped to the entity's role, function and bulk system impact, and every engagement is overseen by a senior practitioner.

WattOps Compliance

Two-story evidence starts when evidence is assembled instead of kept. WattOps Compliance is EC's NERC compliance evidence platform (wattopscompliance.com). EC will run one standard at one facility through WattOps at no cost (CIP standards excluded).

RenewOps

For renewable and storage operators, the operations data is where documentation and practice either match or don't. RenewOps is EC's renewable operations monitoring and analytics platform, with a Data Center module.

If your audit is on the calendar, call before the 90-day notice arrives.

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.

About Energy Compliance, Inc.

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

We support registered entities, including Generator Owners and Operators, Transmission Owners and Operators, Reliability Coordinators, Balancing Authorities, and Distribution Providers. Our work spans 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. We staff for outcomes, not billable hours. Our deliverables are written to be operationally executable and audit-defensible, structured for the auditor's question rather than the consultant's binder. Where automation can replace manual work, we build the automation. Where senior judgment is required, the senior is in the room.

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.

Learn more at energycomplianceinc.com.

Sources and Authorities

- 18 C.F.R. § 385.1602, Civil penalties, as adjusted (eCFR, current as of Oct. 23, 2026; last amended Jan. 14, 2025). https://www.ecfr.gov/current/title-18/section-385.1602
- NERC, Definitions Used in the Rules of Procedure, Appendix 2 to the Rules of Procedure (effective June 27, 2024). https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-2.pdf
- NERC, Sanction Guidelines of the North American Electric Reliability Corporation, Appendix 4B to the Rules of Procedure (effective Jan. 19, 2021), Section 3.3, including Aggravating Factor: Repetitive Violations and Compliance History and Mitigating Factor: Disclosure of the Violation Through Self-Reporting and Voluntary Mitigating Activities by the Entity. https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-4b.pdf
- NERC, Compliance Monitoring and Enforcement Program, Appendix 4C to the Rules of Procedure (effective May 19, 2022), Sections 4.0, 4.1, 4.1.1, 4.1.3.2, 4.5, 5.3, 6.2 and 8.0. https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-4c.pdf
- NERC, Organization Registration and Certification Manual, Appendix 5A to the Rules of Procedure (effective June 27, 2024). https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/appendix-5a.pdf
- NERC, Reliability Standard CIP-002-5.1a, Cyber Security, BES Cyber System Categorization (effective Dec. 27, 2016), Requirements R1 and R2 and Attachment 1. https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-002-5.1a.pdf
- NERC, CIP Reliability Standards listing (status and effective date for CIP-002-5.1a). https://www.nerc.com/standards/reliability-standards/cip
- NERC, ORCP and CMEP Annual Report (Feb. 11, 2026) (2025 data). https://www.nerc.com/globalassets/programs/enforcement/cmep-and-vegetation-reports/2025-orcp-and-cmep-annual-report.pdf

© Energy Compliance, Inc. · EC-WP-105 · October 2026