NERC Audit Definition

- An engagement that provides assurance or conclusions on an evaluation of sufficient, appropriate evidence against stated criteria, such as specific requirements, measures, or defined business practices.
- Specifically for NERC, the objective of the performance audit includes an assessment of the following:
  - Tools
  - Processes
  - Procedures
  - Training Programs
  - Internal Controls
  - Potential and Actual Risk
  - Compliance with Reliability Standards

✓ Program Tips
  ✓ Consider conducting frequent SME briefings
  ✓ Utilize vast archive of internet training resources
  ✓ Conduct internal or mock audits with an outside vendor
FERC/NERC Super Audits

<table>
<thead>
<tr>
<th>Audit Agency</th>
<th>Super Audit</th>
<th>Routine Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>-- FERC</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>-- NERC</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>-- Region</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

Scope

<table>
<thead>
<tr>
<th></th>
<th>Super Audit</th>
<th>Routine Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>-- Actively Monitored List</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>-- Specific Regional Standards</td>
<td>✔</td>
<td>Possible</td>
</tr>
<tr>
<td>-- All Other NERC Standards</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>

Notes on Scope: Actively Monitored List a set of Reliability Standards that are selected based upon NERC-identified high-risk priorities and a three-tiered approach to compliance auditing. The audit scoping process also requires Regional Entities to consider a registered entity’s compliance history when determining the scope of compliance monitoring activities.

Audit Process - Regulatory Players

Regional Regulators

- Audit Team Lead
  - Project Lead and Coordinator
  - Makes final determination of compliance
  - Prepares and presents Audit Open and Exit presentations
- Moderator
  - Ensures additional evidence requests are provided, reviewed, catalogued.
  - Communicates preliminary findings.
- Scribe
  - Documents all evidence
  - Composes Draft Report

- NERC Observer
  - May actively participate and ask questions
  - May submit comments in draft report

- FERC Observer
  - Monitors effectiveness of NERC and Regional
  - Changes the dynamic quite a bit depending on individual
Audit Process - The Initial Notification

1. Audit Notification Letter received 90 days prior to Audit. Includes:
   a) Audit team members biographical information
   b) Non-disclosure information
   c) Pre-audit material
   d) Request for Compliance Data and Documentation
   e) Standards and specific Requirements being audited
   f) Copies of Reliability Standards Audit Worksheets (RSAWs)

   ✓ Pre-Audit Prep Tips
   ✓ Identify all subject matter experts that will be needed.
   ✓ Ensure that propose responses are consistent and clear.
   ✓ Have more than one SME examine each attachment.
   ✓ Prepare the package.
   ✓ Identify Culture of Compliance opportunities.
   ✓ Develop program timeline from initial registration through present day.

Audit Process - Pre-Audit Material Package

1. Region and FERC/NERC requires Entity to submit the pre-audit material at the 45-60 day point. This may include:
   a) Pre-Audit Survey
   b) General Information Questionnaire
   c) Executed Compliance Audit Information Certification Letter
   d) Review all previous Mitigation Plan histories and documentation.
   e) File Transfer Server (EFT).

✓ Pre-Audit Prep Tips (Cont)
✓ Check on skills, qualification and reputation of proposed Regional Audit Team Members.
✓ Develop file naming convention between all internal team members.
✓ Ensure that senior management is involved.
✓ Develop Outlook (calendar) entries for all deadlines.
✓ Plan for Audit Scope creep!
Audit Process- Audit Logistics

1. Ensure that adequate space is available for the audit team.
   a) Two rooms for onsite auditors.
   b) Tours of facilities pre-arranged.
   c) Personnel interviews pre-arranged.
   d) Daily coordination schedule pre-planned.
   e) Daily (evening) management and legal team de-briefings.

Audit Logistic Tips

- Clarify expectations for certifications and attestations.
- Ensure agreement on whether legal or manager presence during interviews is permitted, and rules of engagement, if any.
- Remember to ask auditors lots of feedback and expectation questions.
- Ensure that all written communication is logged as part of the internal audit record.

Audit Process- RSAWs

RSAW Tips

- Don’t forget Technical Feasibility Exceptions while completing RSAWs
- Count on 10-15 hours of total time preparing each RSAW (for everyone)
- Put yourself in the Audit Team’s shoes- what are they thinking about your organization as they review the RSAWs?

1. Reliability Standards Audit Worksheets (RSAWs):
   a) Primary means of submitting mandatory compliance documentation.
   b) An RSAW does not set new requirements for compliance.
   c) Gauge contents against Measures and known compliance attributes from other audited entities.
   d) RSAWs do not limit scope creep by the auditors.
1. Read each RSAW carefully-
version control (of provided
RSAWs) is an issue across
regions and periods.
   a) Follow instructions closely and
      answer ALL inquiries.
   b) Describe the compliance
      procedures clearly.
   c) Describe the internal controls
      that ensure compliance.
   d) Ensure that all Evidence
      references are precise,
      annotated and easy to
      navigate.

---

**RSAW Tips**

- Ensure that all SMEs
  involved with each RSAW
  has reviewed the final
  version.
- Be careful with internal
  version controls- easy to
  submit wrong version.
- Do not append internal
  comments on any drafts-
  use separate comment
  ledger.

---

**Audit Process- RSAW Development**

---

**Audit Process- Evidence Prep**

**Evidence Organization**

   a) Ensure that records conform to a system based on the requisite
      Standard and Requirement.
   b) Records should be easily retrievable for team review.
   c) Do not discard older versions.

**Evidence Quality**

   a) Synching the records to the
      requirements and measures.
   b) Completeness and legibility.
   c) Signed and dated where required.

**Evidence Consistency**

   a) Quality, organization and format
   b) Care to ensure volume consistency.

**Presentation Tips (Onsite)**

- Prepare projector and
  screen beforehand.
- Prepare copies on flash
  drive for auditors
- Remember that auditors
  won’t look for Evidence-
  you must present it.
Audit Process - Culture of Compliance

**Culture Tips**
- Have copies of governance docs, policies and other risk and controls proof.
- Poll multiple levels of your organization for culture “nuggets”.
- Be careful with providing copies of internal audits or assessments - check with counsel first.

1. **Culture of Compliance**
   a) Must be demonstrated at every level of the audit process.
   b) Be cognizant of the sensitivity that regulators have for their authority.
   c) Patiently explain your position and reasons for disagreement with auditors.
   d) Track your culture of compliance through your organization and through your history.

Audit Process - During the Audit

**Communications**
- Designate a single point of contact to interact with the audit team.
- Encourage Regulator SMEs and Entity SMEs to have free exchange of information and ideas.
- Be humble - to the exclusion of over-confidence.

**Readiness**
- Ensure any back-up SMEs are prepped and available “in case”.
- Use lots of flat surfaces and lay out files in sequence of Standards.

**Logistics**
- Bring in lunch - don’t be cheap.
- Volunteer your conference room for post-daily needs by Audit Team.

**Daily Checklist**
- Ensure both Entity and Audit Team Lead maintain daily feedback loop.
- Don’t promise deliverables and then forget. Have extra staff dedicated to immediate discovery and production.
Audit Process- During the Audit (CIP)

Critical Cyber Asset List
a) Be certain that all cyber assets have been categorized appropriately- and the reasons why for each are documented and current.
b) Be very clear about the function of every CCA and all of its attributes: manufacturer, serial #, platform, install dates, custodian, etc. USE MAPS!

✓ Daily Checklist
- Prepare for diverse interpretations of Standards
- Showing consistency and clarity in procedures may substitute for imprecise performance.

CIP-003 (Info Protection and Access Control)
a) Prepare to demonstrate how info is stored and tracked

CIP-005 Access Points
a) Include all configured interfaces
b) Sync with CVA findings

CIP-007 (Systems Security Management)
a) Ensure business justifications are listed for every service listed in your scans

Audit Process- Using Vendors

✓ Vendor Deployment
- Gauge vendor value as a function of what you’re “missing”
- If your internal staff is thin- decide who performs SME and who performs project mgmt.
- Consider using multiple vendors- especially for CIP audits.

1. Selecting Vendors
a) You get what you pay for.
b) Gauge viability by testing expertise against sales msgs.
c) Beware of low hourly rates- many vendors squeeze extra hours.
d) Consider Fixed Price- but be prepared to be transparent about what the Vendor will be facing.
Audit Process - Post-Audit Process

Audit Exit Interview
- NERC will deliver concise statements of possible violations and concerns
- May offer general program improvement suggestions
- May present BES risk statements

Draft Report (30 Business Days)
- Reviews Scope, Methodology, and Internal Control Evaluation
- This Report remains Confidential.
- Entity may offer response and comments.

Final Report (45 Business Days)
- Posted on NERC website
- Corrective Action Plans and Mitigations Plans ensue.

Daily Checklist
- Take notes for future audits
- Review all Audit Team Feedback and implement changes.

Conclusion

- If you’ve waited to prepare for an audit when your audit news arrives, you will probably “fail” the audit.
- The RSAWS are the critical path to communicating your compliance to the auditors.
- Subject Matter Experts will make the biggest difference in the quality of your submittal.
- Culture of Compliance “score” can conceivably overcome issues that might otherwise be violations.
- Prepare for audit day(s) by “choreographing” the agenda, the location, the progress and the interaction (feedback loops).
- Respect the auditors authority and the difficulty of their positions.
- NEVER ARGUE with an auditor.
- Implement mitigation and corrective action plans as if they’ve come from your boss.