

Better Practice Elements for Audit Preparation

David Cerasoli, CISSP

Manager, CIP Audits

John Muir

Director, Compliance Monitoring



This presentation will cover the major milestones of an audit, but it does not include every single step in the audit process. ***When in doubt contact the Audit Team Lead and Primary Auditor assigned to your audit.***

Please send any questions to NPCCCompliance@npcc.org and we will do our best to respond in a timely manner.

We will publish the questions and answers that may be of interest to other entities.

Legend

- Black = CIP and O&P
- Blue = CIP
- Red = Pay Attention

Audit Timeline

Day 0 - Notification Letter with Pre-Audit Survey and Data Request

~Day 10 – Initial Audit Briefing Conference Call

Day 30 – Pre-Audit Submittal and Data Request due

Day 90 – RSAWs and Evidence submittal due (End Day of Audit Period)

Days 90-120 – Auditors review submittal and send requests for additional evidence as necessary.

Day 120 – Start of on-site audit or expected completion date of off-site audit

Day 150 – Draft Report issued - 2 weeks allowed for comments

Day 165 – Comments due

Day 170 – Final Report Issued

Audit Notification Letter

- Your Primary Compliance Contact will receive the audit notification letter at least 90 days before the audit start date.
- Contains Audit Scope and Audit Period
- Outlines milestones and deadlines such as due dates for Pre-audit survey and Initial Submittal
- Provides instructions for data submittals
- Typically includes a pre-audit data request

Audit Kickoff Call

- Typically scheduled by the Primary Auditor within 10 days after the notification letter is sent.
- ***Take advantage of the Initial Audit Briefing to ask any questions you may have about the audit scope, process and the audit team's expectations.***
- Be sure to verify the dates of the various audit milestone to avoid delays in the progress of the audit.

NPCC Drive

- It is a secure Web Portal hosted by NPCC.
- You will upload all your audit submittals to NPCC Drive.
- Your entire submittal should be placed in a single Zip file.
- Give the Zip file a unique name in the format of EntityNameAuditTypeSubmittalDate.
 - Ex: ***ABCGEnCoCIP20170401.zip***

NPCC Drive

While files are being uploaded, there is a small bit of text that reads “Uploading Files”. After your files have been uploaded that text changes to “Uploaded Files”. ***However, the status ring will continue to spin even after your upload has been completed.***

Pre-audit Survey and Pre-Audit Data Request

- Due 30 days after audit notification letter
- With the Pre-audit survey, and all submittals, make sure you verify via e-mail to the Audit Team Lead and the Primary Auditor that the submittals were actually received. ***NPCC Drive has been very reliable, but it's not perfect!***

CIP Pre-audit Survey

- For an on-site CIP audit, you will also be asked to provide four lists:
 - BES Cyber Systems locations with driving distances (or drive times) from audit location
 - List of BES Cyber Systems
 - List of individuals with physical access to BES Cyber Systems
 - List of individuals with electronic access to BES Cyber Systems
- You will be asked if you have any CIP-014 sites. Answer just yes or no.
- Please provide these lists in a spreadsheet format, e.g., MS Excel (.XLS or .XLSX).

O&P Pre-audit Survey

- Additionally, for an O&P audit you will be asked to provide:
 - One-line diagrams of your Facilities, identifying BES Facilities, connections to other entities, etc.
 - For Audits with PRC-005, a list of Protection Equipment in spreadsheet format, e.g. MS Excel.

Pre-audit Survey Submittal

- Submit the Pre-Audit Survey and the responses to the Pre-Audit data requests as soon as possible, but no later than 30 days after the notification letter.
- The Auditors will develop a sample set of the listed data from which we would ask for pertinent evidence (for PRC-005 and CIP-005 for example).
- In order to verify that activity intervals are being respected, we may need evidence that precedes the start date of the audit period.

Initial Submittal

- Due 90 days after the audit notification.
- RSAWs should always be in a Microsoft Word format, e.g., .DOC or .DOCX.
- Policies and procedures should be PDFs, but any lists should be in an Excel format such as .XLS or .XLSX – ***don't save lists as PDFs.***
- Evidence should not be submitted in a format that requires a special client, such as Outlook, to open.
- Do not password protect any evidence.

RSAW and Evidence Preparation

- Provide a detailed narrative in the RSAW for each audited requirement - pay attention to the “Compliance Assessment Approach” for specific things the auditors will be looking for.
- Reference specific sections or appendices in any evidence provided to support compliance.
- Only provide evidence that is relevant, more is not always better. ***If you bury us in evidence then we will have to sort it out while onsite, or submit multiple rounds of data requests, which is generally bad for everyone involved.***

RSAW and Evidence Preparation

- Even when not required by a Standard or Requirement, you should ensure all policies and procedures are signed and dated, and contain a version history.
- If submitting a procedure, also provide evidence that you follow the procedure, e.g., log entry, dated forms or attachments, voice recordings, e-mails, etc.
- *Evidence should be relevant and specific. RSAWs should identify how the evidence demonstrates compliance. Page and paragraph references and annotations help the auditor ensure a smooth audit.*

RSAW and Evidence Preparation

- It would be very helpful if you describe the:
 - Policies and procedures describing actions, studies, tasks to be performed related to the requirement (vegetation management, restoration of power, load shedding, planning studies, etc.)
 - Tools used to carry out these actions, studies, tasks (SCADA, EMS, work management, document management, compliance management, Outlook reminders, etc.)
 - Skilled human capital responsible for carrying out these actions, studies and tasks and/or using the tools (SMEs with relevant training, certified operators, job descriptions, etc.)

RSAW and Evidence Preparation

- If a requirement calls for evidence of an occurrence or an action that didn't happen during the audit period, then provide evidence, such as a procedure or policy, that outlines what you would do if it did happen.
- It is expected that you would provide a description and evidence of how you verified the negative, e.g. reviewed logs.
- This also applies to Requirements that you feel are not applicable.
Provide justification
- An attestation is not required for individual statements in the RSAW. The submittal is certified to be true by completing the "Attestation" document sent with the notification letter.
- Use the NYISO and ISO-NE corroborating evidence guidance documents if applicable (***for example to support your CIP-002 assessment***).

Remote Access to Confidential Evidence

- Consider providing the auditors with remote access to confidential evidence before they come onsite, as it could significantly reduce the amount of time spent onsite.
- ***A secure web portal is ideal***, but a VPN is ok.
- Do not submit **any** confidential evidence for CIP-014.

NP View

- NP View is a tool used to audit firewall rules.
- We will ask you to provide firewall, router, and switch configuration files on a secure laptop. The laptop should be made available when we arrive onsite and will never leave your site.
- The system requirements for the laptop will be reviewed with you during the audit kickoff call.

1st Round Questions

- The audit team will review your initial submittal then send you an Evidence Tracking Spreadsheet (“ETS”) with 1st round questions and/or requests for additional evidence.
- Typically you will receive our 1st round questions two weeks after we receive your initial submittal.

Onsite

- Have security clearance and internet access set up ahead of time to facilitate the on-site process. Once all cleared on the first day, subsequent access should be via credentials provided on first day.
- Provide interview rooms that are large enough to accommodate the number of anticipated attendees.

Onsite

- If possible, interview rooms should be capable of displaying EMS applications and displays. This will minimize the amount of the time the auditors will have to spend in the Control Room.
- Have SMEs clear their schedules as much as possible so that last minute changes to the audit interview schedule can be accommodated – *and those changes happen frequently!*
- Depending on how many BES Cyber System locations and Control Rooms you have, a pre-visit by the audit team may be necessary to complete the audit in a timely manner.

Post Audit

- Your Primary Compliance Contact will receive the draft report within 30 days of the Exit Briefing.
- ***There is a new report format that has resulted in significantly shorter reports. The average CIP report has gone from 80 pages to 12 pages.***
- You will be asked to review the draft report and return any comments within two weeks.
- We will review your comments then issue a final report that will reflect any comments we agree with. Although we usually agree with the comments we receive, ***we are not obligated to update the report to reflect your comments.*** We will discuss with you any comments that we do not agree with before the final report is issued.

Examples of Good and Bad Audit Practices

- **Good:** continuous maintenance of the RSAWs to ensure they reflect current conditions.
- **Bad:** scrambling to update RSAWs after you receive the audit notification letter.
- **Good:** submitting lists in a spreadsheet format such as XLSX.
- **Bad:** submitting lists as PDFs or worse, scanned pictures of lists (yes, it has really happened).

Practice Elements, Cont.

- **Good:** staying in contact with the Primary Auditor and ATL throughout the entire audit process.
- **Bad:** springing things on the audit team when they arrive onsite.
- **Good:** carefully reviewing the on-site audit schedule when it is published in October for any conflicts.
- **Bad:** waiting until after the audit has commenced to tell the ATL that there is a holiday during the week the audit team will be onsite.

Auditor Recommendations

- Review prior audit material, such as Evidence Tracking Sheets, to guide you in developing RSAWs and evidence submittals
- Use a repository to store and control audit evidence and keep it up to date with current evidence
- Treat all Compliance Monitoring activities with the same thoroughness as an audit
- Refer to the Measure associated with each Requirement, the Evidence Requested, the Compliance Assessment Approach, and the Notes to the Auditor sections of the RSAWs for hints to appropriate supporting evidence

Auditor Recommendations

- For evidence that is common to multiple Requirements, include the evidence for each Requirement in each individual audit folder.
- Refer to the Measure associated with each Requirement, the Evidence Requested, the Compliance Assessment Approach, and the Notes to the Auditor sections of the RSAWs for hints to appropriate supporting evidence.

Follow up

- Any questions that are submitted for this WebEx will either be answered directly or published in a document that will be made available on our website.

NPCCCompliance@npcc.org

- Thank you for your participation.