Network &Security Technologies
Voice (845) 620-9500 Fax (845) 512-2093
http://www.netsectech.com

NERC CIP MOCK AUDIT

NERC CIP MOCK AUDIT

Identifying when a NERC CIP Mock Audit may be right for you

Many entities struggle to demonstrate compliance with NERC CIP Security Standards. Common issues include:

- Reliability Standard Audit Worksheets (RSAWs) with unfocused or irrelevant verbiage, or that only rehash Requirements or statements pulled from the entity's security policy, rather than offer a clear roadmap of the controls and documentation provided,
- SMEs unprepared for the GAGAS "show me the evidence" style of questioning,
- Inconsistent procedures and technical controls across business units (power, IT, physical security), and
- Irrelevant or excessive documentary evidence provided to demonstrate compliance.

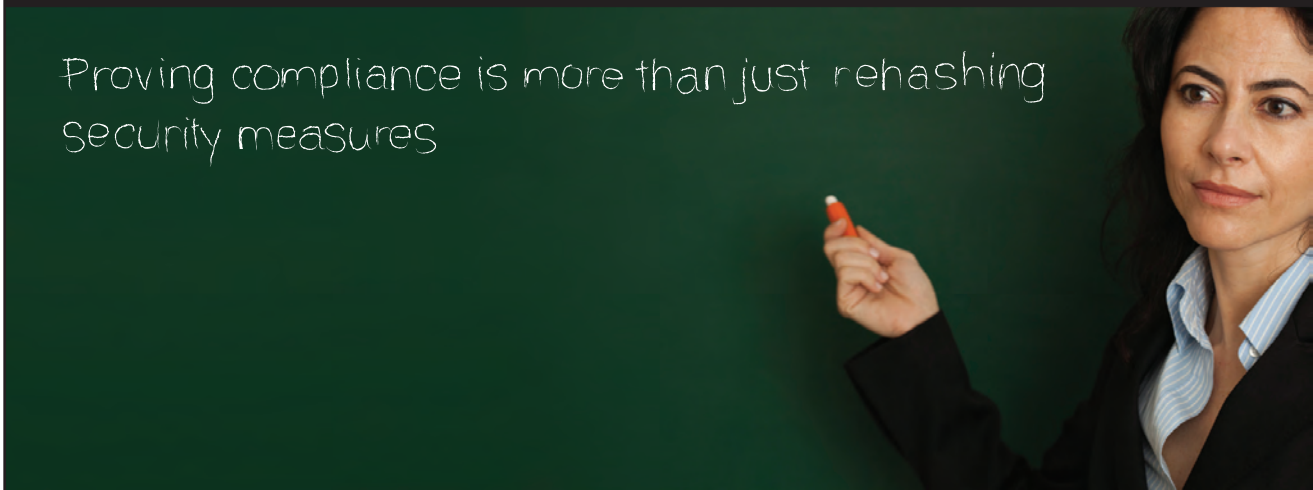
Such issues can lead to a difficult NERC CIP audit characterized by lengthy and potentially unresolved lines of questioning, numerous after-business hours devoted each night to fulfilling data requests, and having areas unnecessarily deemed non-compliant.

N&ST's approach: Confidence Comes with Practice

N&ST has developed an offering to assist an entity in becoming better prepared for its NERC CIP Audit by its Regional Entity (RE). Led by two senior consultants with direct experience working with REs, both on and off official Audit Teams, the engagement follows the general approach and format of an official audit. Sessions interleave coaching discussions with SMEs regarding strategies, tactics, and targeted wording to use in response to auditor questioning. Thus, the SMEs will become prepared in responding to questions and discussing their evidence in a manner that facilitates the goal of the Audit Team: to determine compliance. During the engagement all 43 requirements in the eight Standards (CIP-002-009) are evaluated, although ad hoc coaching advice, discussion around particular SME responses, as well as a need for prolonged focus on certain requirements, may limit deep analysis of all Requirements or a Standard as a whole.

N&ST encourages representatives from Internal Audit and Legal, in addition to the core NERC CIP compliance team and SMEs, to participate in the Mock Audit to become familiar with the style of questioning and the burden of proof on the organization.

"WILL I PASS THE NERC CIP AUDIT?"



Voice (845) 620-9500 Fax (845) 512-2093
http://www.netsectech.com

NERC CIP MOCK AUDIT DRESS REHEARSAL

THE DRESS REHEARSAL

N&ST begins the engagement – a rehearsal for the actual audit – by reviewing the entity's RSAWs and other evidence they intend to present for compliance determination. SME interviews are conducted to simulate the GAGAS approach, using the RSAW to guide the questions and interpret other evidence. Sessions are started with an "auditor hat on", unless issues arise during the interview, such as inappropriate verbiage, volunteering information, or "deer in headlights" occasions, that would initiate "hats off" discussions. The line of questioning may reveal the need to make changes to the materials provided as evidence – additions, modifications, and even removal of irrelevant items. Inconsistencies in policy, process, procedures, and evidence across responses from the power, IT, and physical security SMEs will be discussed with the group, noted and recorded by the entity, and captured in the workbook created by the N&ST consultants to log evidence presented. At the conclusion of the interview portion of the engagement, SMEs should be better able to convince the Audit Team that the entity practices what is documented. They will do this by "painting a picture" of policy impact, enacted procedures, and implemented controls intended to reduce unauthorized access.

N&ST will deliver two documents at the conclusion of the engagement. The first is a workbook listing observations, compliance opinion, and recommendations for each individual Requirement in the Standards. The other is a presentation summarizing the findings and recommendations, as well as some reminders for preparing for the audit.

The lessons learned during the "dress rehearsal" should result in an audit characterized by workdays ending at a reasonable hour, a small number of data requests, and SMEs not so drained they cannot return to their desks and work. Most of all, there should not be any surprise "Potential Violations" beyond known gaps in controls. In some cases, a low-anxiety audit may lead to free advice from the RE Audit Team.

OPTIONS TO CUSTOMIZE THE MOCK AUDIT TO YOUR SPECIFIC NEEDS

There are three optional modules that may be incorporated into the Mock Audit to ensure that it is custom tailored to address the individual needs of the entity:

- **SME Workshop:** Some SMEs, frequently the more technically proficient, have never participated in any type of audit. N&ST has developed a one-day workshop to introduce these SMEs to the audit experience. Role play exercises have been developed to simulate actual lines of questioning, and to demonstrate behaviors SMEs should exhibit when in front of the RE Audit Team. This workshop is best placed at the start of the engagement, ensuring that the SMEs are better prepared for the "auditor hats on" interviews that will be conducted as part of the Mock Audit.
- **Document (Re)writing:** Once the interviews have been completed, the entity may desire assistance in writing or updating the RSAWs. Well written responses in these documents should guide the Audit Team to understand the programs, controls, and evidence provided for compliance determination by painting a picture of the overall program and materials provided. These responses should present unified approaches that may be implemented separately by the power, IT, and physical security business units. Additional types of documents may also be reviewed and edited by the N&ST consultants, such as policies, programs, and procedures.
- **Individualized SME Coaching:** During interview sessions, N&ST and/or members of the entity's business units, may flag certain SMEs requiring additional coaching. Either in a small group setting or one-to-one, N&ST will work with these SMEs to practice interview skills to become more relaxed and proficient at handling ad hoc questions in an intuitive manner.

Voice (845) 620-9500 Fax (845) 512-2093
http://www.netsectech.com

CONSTRUCTING THE NERC CIP MOCK AUDIT

CONSTRUCTING THE MOCK AUDIT

Goals:

- Determine level of compliance with the NERC CIP Security Standards
- Prepare SMEs for audit experience
- Identify and package relevant documentation as evidence

Core Activities:

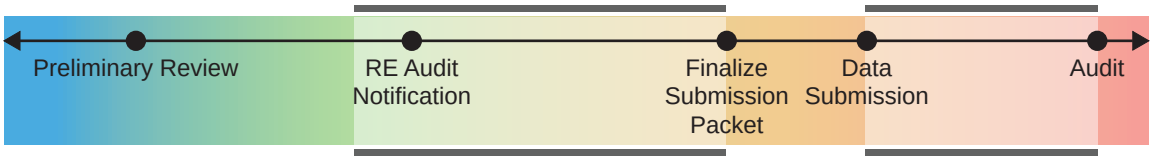
- Review initial package, including RSAWs and other evidence
- Interview and coach SMEs
- Identify and analyze documents for submission to the RE
- Deliver workbook of compliance opinion and Mock Audit presentation

Accompanying Options:

- *One day SME training workshop:* Introduce staff, mostly technical, to the audit experience, interview environment, and behaviors to master to streamline responding to questions. If selected, this session should occur the first day of the on-site activities.
- *Document (Re)writing (up to 16 hours):* Assist in (re)writing RSAWs, policy, program, and procedural documentation.
- *Additional Training (up to 16 hours):* Conduct individual and/or group interview sessions with flagged SMEs to further develop their skill in handling the audit environment and style of questioning. In addition, meet with members of Internal Audit to advise them on how to make a NERC CIP program, and evidence generation and retention processes, permanent.

Recommended Timing:

Best results occur if the Mock Audit is scheduled to occur prior to or in conjunction with development of entity response to the initial data requests from the RE (RSAWs, initial evidence workbooks, and samples). Once the RSAWs and evidence workbooks have been submitted to the RE, those materials cannot be changed. In that case, the focus of the Mock Audit would be on SME interviews, role play, and coaching.



SAMPLE SCHEDULE FOR THE MOCK AUDIT

Core Schedule

Week/Day	M	T	W	T	F
1: Off-Site	Doc Review & Questions	Doc Review & Questions	Doc Review & Questions	Doc Review & Questions	Doc Review & Questions
2: On-Site	CIP-002 CIP-008 CIP-009	CIP-003 CIP-004	CIP-004 CIP-006	CIP-006	Tours
3: On-Site	CIP-005	CIP-005 CIP-007	CIP-007	CIP-007	Mock Audit Presentation

With Optional Sessions

Week/Day	M	T	W	T	F
1: Off-Site	Doc Review & Questions	Doc Review & Questions	Doc Review & Questions	Doc Review & Questions	Doc Review & Questions
2: On-Site	SME Workshop	CIP-002 CIP-008 CIP-009	CIP-003 CIP-004	CIP-004 CIP-006	CIP-006
3: On-Site	Tours CIP-005	CIP-005	CIP-005 CIP-007	CIP-007	CIP-007
4: On-Site	Document Writing	Document Writing	SME 1-on-1	SME 1-on-1	Mock Audit Presentation

Voice (845) 620-9500 Fax (845) 512-2093
http://www.netsectech.com

NERC CIP MOCK AUDIT CASE STUDY

CASE STUDY

N&ST recently conducted a Mock Audit for an entity operating as a generation and transmission operator with a NERC CIP audit scheduled to occur during the month of May. The Mock Audit occurred during the end of February / beginning of March 2012, a bit more than two months prior to the actual audit. The Entity received its package from its RE in mid-February, with the expectation that completed RSAWs, evidence workbooks, and samples would be delivered in the first half of March.

The two consultants on the engagement both worked in the past directly with at least one RE, one on multiple NERC CIP audits, the other on spot audits and enforcement activities. Their familiarity with the practices and schedules of actual audits enabled them to run the Mock Audit as closely as practical to a real one. With only two consultants, rather than six or more RE, NERC, and FERC auditors divided into two teams, the consultants were not able to examine the full breadth the documentation or interview the SMEs to the same level of detail, yet were able to acquire sufficient information to both simulate an audit and render compliance opinions.

At the start of the engagement, a schedule was set, including the off-site review of available documents, such as RSAWs, policies, program materials, procedures, and other evidence. During the first week on-site, the consultants conducted interviews with SMEs to evaluate the controls for CIP-002, CIP-003, CIP-004, CIP-006, CIP-008, and CIP-009, as well took tours of several local facilities. The two more technical Standards, CIP-005 and CIP-007, were addressed during the second week on-site. On the final day, a presentation was delivered to those who participated directly in the interviews as well as managers of those groups, including the NERC CIP compliance team and representatives from Internal Audit and Legal.

- **One key to the success of the engagement was the manner in which the interview sessions were conducted.** All interviews commenced with the setting of ground rules. In particular, the sessions would involve both “hats on” and “hats off” episodes in which the N&ST “auditors” would quickly change demeanor from NERC CIP auditors behaving in character to consultants offering advice on responding to the line of questioning. The mixing of interviewing and coaching was instrumental in preparing the SMEs as well in determining the level of compliance with individual Requirements.

- **A second key to the success was the mixture of participants.** In addition to the subject matter experts, members of the entity’s NERC CIP program, Internal Audit, and Legal participated in most, if not all, sessions. As the “hats on” / “hats off” episodes unfolded, those in the room other than the SMEs were able to assimilate the experiences into notes for updates to documentation, coaching notes for SMEs, and the presentation of evidence. The role for the representative from Legal as “bad cop” during the actual audit was discussed to ensure that this discipline should only be used selectively and only when truly necessary to keep the actual audit on track.

- **The final key to the success was the real-time response by the entity to the data requests and other communications with the RE.** All members of the entity team were able to discuss nuances of the data requests, in particular the logic of the sampling requests and tactics for packaging and presenting that information. The N&ST consultants used their experience with audits to determine the logic behind the sample from the RE. N&ST was also able to advise the entity on how to package the various types of evidentiary files for submission.

Voice (845) 620-9500 Fax (845) 512-2093
http://www.netsectech.com

NERC CIP MOCK AUDIT CASE STUDY

CASE STUDY CONTINUED

At this particular entity, there were approximately twelve SMEs in addition to the core group responsible, directly or indirectly, for the NERC CIP compliance program. During the initial interview sessions there were many cases in which the entity stumbled to provide logical, coherent responses to the N&ST auditors' questions. While they believed they were familiar with their controls and documentation, the SMEs had never explained their policies, programs, and procedures to those well versed in asking probing questions and generally unfamiliar with them. Gaps between responses from silo'd teams were readily apparent to all in the room. Similar experiences occurred when evidentiary records were presented for review. Caucus sessions were used by the N&ST consultants to offer advice to the SMEs in phrasing and structuring responses to effectively convey their feelings. Other members of the entity's NERC CIP team were likewise advised on changes to make to various types of documents, including the RSAWs. In a few cases, lines of questioning were repeated to enable the SMEs to incorporate new tactics and information. As the days passed, all of the SMEs became much more confident in responding to and addressing each aspect of the questions posed. They became practiced at tailoring responses to avoid information extraneous to the topic being addressed by auditors in order to minimize areas auditors could investigate.

A notable output of the engagement was advice for scheduling SMEs for the interview sessions with the RE Audit Team. In particular, the entity was encouraged to ensure that interview sessions assessing technical controls should have one manager and one subordinate intimately familiar with the technology, procedures, and settings. This pairing ensures that questions at all levels are addressed, including managerial commitment to identifying another SME with the specific knowledge. This pairing also distributes responsibility for being "on the hot seat" over a larger number of people, reducing the demands on specific SMEs.

The entity worked with N&ST to perform a complete rewrite of the responses for one RSAW. The N&ST consultants encouraged the entity to replace most of its text with focused responses. Generalizations about the organization's Cyber Security Policy were replaced with text addressing the tenets of the requirement, statements about similarities and differences in processes across the silo'd teams, the few TFEs already submitted to the RE, and spare mention of controls above those mentioned in the Standards. All members of the entity's NERC CIP program understood the value of the new responses in light of the challenging auditor questions and informal consultant-led discussions.

As SMEs cycled through the interviewing room, the N&ST consultants were able to provide additional information about the auditing experience, such as room arrangement, roles and responsibilities of staff, the use of caucus sessions, SME mindset, and other behaviors to support a smoothly conducted interview.

The benefits of the Mock Audit are expected to persist. The NERC CIP team will use the new RSAW responses as a model to update the other RSAWs. The SMEs will be prepared through the review of copious notes taken by all who participated in the engagement. At the end of the engagement Internal Audit met with the N&ST consultants to inquire about the best tactics for supporting the rigor of their NERC CIP efforts, incorporating these ideas into their plans. Internal Audit expects to review evidentiary materials beginning in the fall for persistence and quality of information. The Legal representative will provide assistance in SME preparations for the audit in May.

"We have never been in a situation where our SMEs ask for the same consultants again and again, until working with your team!"
-Case Study Entity Testimonial

Network &Security Technologies
161 North Middletown Road, Pearl River, NY. 10965