



# NERC Provides Best Practices for Effective Procedures

*Deborah A. Carpentier*

**T**he North American Electric Reliability Corporation (NERC) recently issued a report of its findings after analyzing the auditing procedures of its eight regional entities, related to the disturbance event reporting standards: CIP-001-2a, EOP-004-1, and EOP-004-2.<sup>1</sup> While an auditor must perform the due diligence necessary to have a reasonable assurance that a responsible entity (an entity responsible for compliance with a particular reliability standard) is in compliance with a standard, inevitably different compliance auditing practices are used across the eight regions. Such inconsistency could lead to different results.

Through its Key Reliability Standard Spot Check program, NERC analyzes compliance auditing practices to identify these areas of inconsistency and auditing practices that might require improvement to ensure consistent, effective, and rigorous compliance audits. In its report, NERC analyzed CIP-001-2a (sabotage reporting) because it was in effect for a full year and has been a highly violated standard. In addition, NERC analyzed EOP-004-1 (disturbance reporting) because responsible entities

often use the same procedures for addressing EOP-004-1 and CIP-001-2a. While CIP-001-2a and EOP-004-1 are retired as of December 31, 2013, they are replaced by EOP-004-2 (event reporting), and the report provides guidance on auditing practices the regional entities should use in the future with respect to that standard.

Several of the best practices highlighted in the report focus on the appropriateness (quality) and sufficiency (quantity) of evidence necessary to demonstrate compliance and are relevant to reliability standards in general, not just to event reporting standards. Moreover, while the report is generally directed to auditors, responsible entities will be better equipped to demonstrate compliance if they maintain and present evidence that will meet the auditor's evidentiary standards discussed in the report.

### USE OF PROCEDURES AS EVIDENCE

Many reliability standards require that a responsible entity have a procedure in place for performing a particular task. For example, CIP-001-2a requires that a responsible entity "have procedures for the recognition of and for making their operating personnel aware of sabotage events," and EOP-004-2 requires a responsible entity to have an event reporting operating plan for reporting specified events to relevant authorities.

NERC found that procedures provided as evidence often were not satisfactory to demonstrate compliance.

### Procedures Must Be Valid

While NERC and the regional entities have stated in compliance conferences and elsewhere that

**Deborah A. Carpentier** ([dcarpentier@crowell.com](mailto:dcarpentier@crowell.com)) is a counsel in Crowell & Moring LLP's Environment, Energy & Resources Group. She focuses primarily on federal regulatory and transactional energy issues for electric utilities in matters before the Federal Energy Regulatory Commission and the North American Electric Reliability Corporation. This article is provided by Crowell & Moring LLP only for educational and informational purposes and is neither intended as nor should it be construed as legal advice. This article may be considered advertising under applicable state laws.

a procedure must include a title, purpose, revision level, revision history, effective dates, review date, approval, and an authorizing signature,<sup>2</sup> or any other attributes that would signify the quality of evidence that would be satisfactory to demonstrate compliance, called “appropriate evidence,” it appears that procedures might continue to lack these attributes.<sup>3</sup> Therefore, NERC recommends that regional entities follow Chapter 6 of the Generally Accepted Government Auditing Standards (GAGAS),<sup>4</sup> which covers evidence validation, whenever accepting procedures as evidence of compliance.<sup>5</sup>

Although NERC is not specific as to the elements of GAGAS Chapter 6 that are instructive in this regard, under GAGAS, for evidence to be of an acceptable quality, it must be valid. “Validity refers to the extent to which evidence is a meaningful or reasonable basis for measuring what is being evaluated.”<sup>6</sup> NERC presumably requires a procedure to have the listed attributes to signify, for example, that the procedure is an official document of the responsible entity, that it was not created just before the audit to satisfy the requirement but rather is a procedure that was in place during the entire audit review period, and that it is a document that changes over time depending on changes in standards or operations.

Thus, the listed attributes give the procedure validity as evidence to demonstrate compliance with a standard requiring such a procedure.

### **Corroborating Evidence Is Needed for Procedures**

NERC also found circumstances in which a responsible entity had a requisite procedure, but appropriate personnel were unaware of the existence of such procedure, or if they were aware, either did not understand the procedure or did not know how to find the procedure. Therefore, NERC concluded that the existence of the requisite procedure alone (whether in hard copy or electronic format) is insufficient to demonstrate that appropriate personnel are provided guidance about its content,<sup>7</sup> and recommended that an auditor require corroborating evidence, such as the following:

- Emails to appropriate personnel advising as to the location and nature of the procedure
- Records of personnel training on the procedure

- A documented response from appropriate personnel that they have read and understand the procedure
- A request that an individual required to have been provided guidance on a procedure demonstrate to the auditor that the individual knows where the procedure is located and guide the audit team through the procedure to demonstrate that such individual understands the procedure<sup>8</sup>

NERC also advised that where a responsible entity only provides its personnel with electronic versions of a procedure, the entity should make a hard copy accessible if access to electronic documentation was lost.<sup>9</sup>

Beyond these evidentiary requirements for the use of procedures as evidence, a responsible entity, in general, needs to understand all of the standards by which auditors will judge the appropriateness and sufficiency of its evidence.<sup>10</sup> Thus, personnel responsible for maintaining evidence and demonstrating compliance would be well served in understanding the evidentiary concepts set forth in GAGAS Chapter 6 so that the responsible entity maintains the right kind of evidence to successfully demonstrate compliance.

### **ATTESTATIONS MUST BE CORROBORATED**

Generally, an assertion of compliance is not sufficient to demonstrate compliance with a reliability standard. Therefore, NERC requires objective evidence to corroborate an assertion so that an auditor can be reasonably assured that a responsible entity is compliant with a particular standard.

Several of the NERC reliability standards require that a responsible entity take certain action upon a triggering event. For example, EOP-004-1 requires that a responsible entity “experiencing a reportable incident shall provide a preliminary written report to its Regional Reliability Organization and NERC,” and EOP-004-2 has a similar requirement. If a reportable incident occurs during an audit review period, evidence to demonstrate compliance is readily available in the submitted report. However, there is no similar evidence available if no reportable incident occurred.

Because of the challenges associated with proving the negative, auditors have instead allowed

a responsible entity to provide an attestation that no such triggering event occurred. But the regional entities have used different criteria for the acceptance of and dependence on such attestations as evidence. For example, auditors have accepted signed letters from corporate officers indicating that no event occurred during the audit review period that would have triggered the requirement, or the provision of the same assertion in the reliability standard audit worksheet (RSAW), which is a document that must be prepared by the responsible entity and submitted to the audit team prior to an audit.

NERC makes several recommendations to promote compliance audit consistency. While these are directed toward the regional entities, a responsible entity also should incorporate the recommendations into its compliance program so that its future attestations will be accepted as evidence. First, NERC recommends that corroborating evidence be obtained when a responsible entity seeks to rely on an attestation as evidence.<sup>11</sup> NERC notes that such evidence could include operating logs, interviews with subject-matter experts, and the review of available event information.

However, if no triggering event occurred, the question becomes how much of this corroborating evidence will be needed to demonstrate compliance. Of particular concern is whether inordinate efforts will have to be made in gathering and presenting corroborating evidence if the responsible entity truly has to prove the negative. For example, operator logs are unlikely to affirmatively state that no EOP-004 triggering event occurred.

Subject-matter experts will still only be able to make the assertion that no triggering event occurred, and unless all event information for the audit review period was reviewed and analyzed to see if any event would have involved the responsible entity at issue, it is not clear what evidence could be gained from available event information. Thus, NERC should provide some additional guidance on what an auditor is to glean from such corroborating evidence and how much of such evidence will be required to demonstrate compliance. Without this further guidance, there is a potential for further divergent approaches among the regional audit teams.

Second, NERC recommends that all attestations should be signed by a subject-matter expert with “intimate knowledge of the event being attested,” which is reasonable.<sup>12</sup> Third, NERC will continue

to allow auditors to accept RSAWs as attestations so long as the attestation is “clearly defined, covers all elements of the requirement,” and is signed by a subject-matter expert as noted.<sup>13</sup> A question relative to these two signature requirements is whether the subject-matter expert has the authority to make such an attestation on behalf of a responsible entity (for example, if the subject-matter expert is a contractor). Thus, a responsible entity should consider whether its own internal processes should require a signature from not only the subject-matter expert, but also a corporate official who oversees the subject-matter expert.

A responsible entity should consider whether its own internal processes should require a signature from not only the subject-matter expert, but also a corporate official.

Finally, NERC recommends that the regional entities develop formal written procedures regarding the acceptance of attestations. NERC should clarify that these procedures, when developed, should be accessible to all responsible entities so that they can incorporate them into their own audit-preparation processes and knowledge base. 

## NOTES

1. NERC. (2013, December). *Key reliability standard spot-check report: CIP-001-2a, EOP-004-1 and EOP-004-2*. Retrieved from <http://www.nerc.com/files/PRC-005-1%20KRSSC%20Final%20Report-%2009142011.pdf>.
2. See, e.g., Carpentier, D. (2011, April). Demonstrating compliance with NERC reliability standards. *Natural Gas & Electricity*, 27(9), 5 and Note 8.
3. See Note 1, at 15.
4. See Comptroller General of US. (2011, August). *Government Auditing Standards 2011 Internet version*. Retrieved from <http://www.gao.gov/govaud/iv2011gagas.pdf>.
5. *Ibid.*, paragraphs 6.56 through 6.72.
6. *Ibid.*, paragraph 6.60.
7. See Note 1, at 16–17.
8. *Ibid.*, 17.
9. *Ibid.*
10. Under GAGAS, “[a]ppropriateness is the measure of the quality of evidence that encompasses its relevance, validity and reliability in providing support for [an auditor’s] findings and conclusions,” and “[s]ufficiency is a measure of the quantity of evidence used to support [such] findings and conclusions”—i.e., whether the responsible entity has provided enough evidence to demonstrate compliance. GAGAS, paragraph 6.57.
11. See Note 1, at 15.
12. *Ibid.*
13. *Ibid.*