

# NERC

NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

## NERC Regional Entity Audit Of Reliability *First* Corporation

Prepared by Jacqueline Power

to ensure  
the reliability of the  
bulk power system

116-390 Village Blvd., Princeton, NJ 08540  
609.452.8060 | 609.452.9550 fax  
[www.nerc.com](http://www.nerc.com)

## Table of Contents

---

Chapter 1 – Executive Summary .....	1
Overview .....	1
Best Practices (for Consideration) .....	2
Lessons Learned.....	3
Chapter 2 – Background .....	4
Basis .....	4
Program Development .....	4
Chapter 3 – Audit Process .....	6
Compliance and Certification Committee Participation .....	6
Pre-Audit.....	6
On-Site Process .....	6
Chapter 4 – Financial and Budget Management.....	8
Background.....	8
Discussion of Review .....	8
Conclusion .....	8
Chapter 5 – Information Systems .....	9
Discussion of Review .....	9
Conclusion .....	10
Chapter 6 – Compliance Audit Validation .....	11
Discussion of Review .....	11
Conclusion .....	11
Appendix A – AUP Exceptions to the Rules of Procedures, Delegation Agreement and Other .....	12
Data Retention and Confidentiality .....	12
Independence .....	12
Reporting to NERC.....	12
Compliance .....	13
Registered Entity Reporting.....	14
Investigations .....	15
Penalties, Sanctions, and Settlements .....	15
Mitigation Plans .....	15
ERO Functional Requirements .....	15

Table of Contents

---

Appendix B – AUP Exceptions ..... 17

    Data Retention and Confidentiality ..... 17

    Independence ..... 17

    Registration ..... 18

    Compliance ..... 19

    Investigations ..... 20

    Mitigation Plans ..... 20

    ERO Functional Requirements ..... 20

Appendix C – AUP Procedures List ..... 21

## Chapter 1 – Executive Summary

---

### Overview

In accordance with the Federal Energy Regulatory Commission’s (FERC) Order No. 672, the North American Electric Reliability Corporation (NERC) developed a program to audit the Regional Entities’ adherence to the Rules of Procedures (ROP), the Compliances Monitoring and Enforcement Program (CMEP) and the requirements of the Regional Delegation Agreement (RDA). This effort was pursuant to FERC’s direction contained in Paragraph 773.<sup>1</sup> Additional requirements concerning the Regional Entity Audit Program attributes are contained in the ROP Section 402.1.3.<sup>2</sup>

Based on the NERC Board of Trustees’ (BOT) recommendation, NERC partnered with an independent auditing firm, Crowe Horwath, LLP (Crowe) to develop the procedures and perform the Regional Entity Audit Program. NERC determined an Attestation of Agreed-Upon Procedures (AUPs)<sup>3</sup> was the best vehicle for meeting its responsibility as outlined by FERC. The Crowe endeavor was coupled with NERC staff performing areas requiring technical subject matter expertise.

NERC staff performed assessments in the following three areas: 1) information systems (Regional Entity processes for maintenance and control of data security); 2) audit validation (validation of the results of a compliance audit performed by the Regional Entity on one of its registrants); and 3) financial and budget management (a review of the Regional Entity’s financial records).

---

<sup>1</sup> See *Rules Concerning Certification of the Electric Reliability Organization; Procedures for the Establishment, Approval and Enforcement of Electric Reliability Standards*, FERC Stats. & Regs., ¶ 31,204 at P 773 (“Order No. 672”), *order on reh’g*, FERC Stats. & Regs. ¶ 31,212 (2006) (“Order No. 672-A”) (“We contemplate that a compliance audit of the ERO would typically involve an examination of the ERO’s ongoing compliance with statutory and regulatory criteria for certification and its performance in carrying out its responsibility to oversee the compliance with and enforcement of Reliability Standards. The Commission, however, maintains the flexibility to determine the applicable scope of a particular audit. The Final Rule eliminates the proposed periodic Commission compliance audit of each Regional Entity. Instead, we require the ERO periodically to audit each Regional Entity’s ongoing compliance with relevant statutory and regulatory criteria and performance in enforcing Reliability Standards and report the results to the Commission.”).

<sup>2</sup> See NERC Rules of Procedure at § 402.1.3 (“Regional Entity Program Audit - At least once every three years, NERC shall conduct an audit to evaluate how each regional entity compliance enforcement program implements the NERC Compliance Monitoring and Enforcement Program. The evaluation shall be based on these rules of procedures, the delegation agreement, approved regional entity annual compliance enforcement program annual implementation plans, required program attributes, and the NERC compliance program procedures. These evaluations shall be provided to the appropriate ERO governmental authorities to demonstrate the effectiveness of each regional entity.”).

<sup>3</sup> An Attestation of an Agreed-Upon Procedure is an engagement relating to Agreed-Upon Procedures (criteria for auditing) to specified elements or accounts. Agreed-Upon Procedures are an engagement with an accounting firm that is hired to issue a report of findings (attestation) based on specified criteria. The user of the report, in this case NERC, agrees upon the procedures to be conducted by the accountant that NERC believes are suitable to the requirements. NERC takes responsibility for the adequacy of the procedures. In this engagement, the accountant does not express an opinion or negative assurance. Instead, the report is in the form of procedures and findings.

The audit of ReliabilityFirst Corporation's (ReliabilityFirst) adherence to its delegated functions was held at ReliabilityFirst headquarters during the weeks of March 23, 2009 and March 30, 2009. Two observers from FERC representing the Office of Electric Reliability (OER) and the Office of Enforcement (OE) were present for the audit. A Compliance and Certification Committee (CCC) representative from Georgia System Operator Corporation participated as an observer for the first week of the audit.

ReliabilityFirst staff was very accommodating to the needs of the audit team. ReliabilityFirst provided all pre-audit information requested on or before the due date. In addition, ReliabilityFirst worked diligently to provide supplemental information requested by the audit team.

There were 43 exceptions to the AUPs criteria noted, of which 22 were identified as exceptions to stated requirements. The attestation of the AUPs performed by Crowe is provided in a separate report.

Appendix A and B of this report contain the exceptions to the AUPs noted by Crowe: Appendix A includes exceptions relating to non-adherence to the ROP, Delegation Agreements, or other NERC guidance or direction documents; Appendix B includes exceptions that do not necessarily constitute non-adherence to the ROP and Delegation Agreements. For example, per the NERC CMEP § 3.4.1, Compliance Violations Investigation Process Steps, a Regional Entity is required to report to NERC within two business days its decision to initiate a compliance violation investigation; however, documentation of its assessment and determination to initiate the investigation is not required. The lack of documentation in this example makes it difficult for the auditors to determine adherence to the requirement. From an auditing perspective and based on the American Institute of Certified Public Accountants (AICPA) standards, it is clear an action was performed when there is documentation of the action, i.e., a checklist, sign-off with date specified, etc., and subsequent documentation that the entity met its timeline.

There were no deficiencies noted by NERC staff in the areas of information systems, compliance audit validation, or ReliabilityFirst's financial and budget management. Further details regarding each area assessed by NERC are contained in subsequent sections of this report.

### **Best Practices (for Consideration)**

As this is the first Regional Entity audit, classification of a best practice is somewhat premature and difficult to designate. However, the NERC audit team noted several areas in which items should be considered as a potential Regional Entity best practice.

#### **ReliabilityFirst Data Security:**

ReliabilityFirst has a professional and responsive information security organization. Interviews with other staff members indicated that the organization is quick to address the needs of ReliabilityFirst staff and the member companies within its footprint. ReliabilityFirst takes great pride in the upgrades made to its data equipment infrastructure.

These upgrades have increased the effectiveness of its monitoring and control over the security of its data. The NERC audit team noted the following key areas.

- All information security personnel are trained in the requirements of NERC’s Critical Infrastructure Protection (CIP) Reliability Standards.
- Reliability*First* has made a significant investment in its data infrastructure. For example, Reliability*First* has upgraded its infrastructure to replace several legacy systems inherited from three previous “Regions” combined into the formation of Reliability*First*.
- Reliability*First* devised a simple but secure off-site storage process that does not rely on third-party contractors.

### **Audit Components**

Reliability*First* uses an auditor’s checklist as an aid in meeting key timelines and steps associated with information required prior to, during and after each compliance audit.

### **Lessons Learned**

At the conclusion of the audit, NERC met with Reliability*First*’s executive management and staff to identify Regional Entity audit process improvement items for NERC to consider. Reliability*First* offered a number of suggestions to improve the overall process. One significant challenge identified was associated with the time the audit team was onsite. Two consecutive weeks at the Reliability*First* offices resulted in intensive support from Reliability*First*’s staff as well as for the audit team. Based on this experience, scheduling of the next Regional Entity audit will include a week off-site and a week on-site.

## Chapter 2 - Background

---

### Basis

In accordance with Order 672 of FERC, NERC developed a program to audit the Regional Entities' adherence to the NERC ROP and the Delegation Agreements. This effort was pursuant to FERC direction contained in Paragraph 773.<sup>4</sup> Additional requirements concerning the RE audit program attributes, including timelines, are contained in the ROP, Section 402.1.3.<sup>5</sup>

### Program Development

NERC Compliance staff solicited proposals from four well-known, publicly recognized auditing firms. Three engagement types were provided by the auditing firms: 1) consultative; 2) management assertion; and 3) attestation of AUPs. NERC executive management and the Compliance staff responsible for the project met on numerous occasions to discuss the options provided. An attestation of AUPs was determined the best vehicle to use for implementation of the NERC Regional Entity Audit Program as this type of engagement provides an audit format which is not open to subjectivity, and can be consistently applied.

Also, NERC contracted Crowe to develop a consulting report in the form of a management letter to identify any areas of process improvement noted during the development of the AUPs (management letter to NERC) and for each subsequent Regional Entity audit (management letter for each Regional Entity).

Jacqueline Power, a NERC Senior Regional Entity Compliance Program Auditor, worked with Crowe staff and the NERC program owners to develop the AUPs criteria. A listing of the AUPs references is captured in Appendix C.

Based on requests from the Regional Entities, NERC executive management determined to include other areas related to the Regional Entity's ERO functional requirements to the program during the first cycle of audits.<sup>6</sup> The decision was based on reducing the burden placed on the Regional Entities for supporting two separate audits.

---

<sup>4</sup> Order 672, ¶ 773. We contemplate that a compliance audit of the ERO would typically involve an examination of the ERO's ongoing compliance with statutory and regulatory criteria for certification and its performance in carrying out its responsibility to oversee the compliance with and enforcement of Reliability Standards. ... The Commission, however, maintains the flexibility to determine the applicable scope of a particular audit. ... The Final Rule eliminates the proposed periodic Commission compliance audit of each Regional Entity. Instead, we require the ERO periodically to audit each Regional Entity's ongoing compliance with relevant statutory and regulatory criteria and performance in enforcing Reliability Standards and report the results to the Commission.

<sup>5</sup> Rules of Procedure, Section 402.1.3 - Regional Entity Program Audit - At least once every three years, NERC shall conduct an audit to evaluate how each regional entity compliance enforcement program implements the NERC Compliance Monitoring and Enforcement Program. The evaluation shall be based on these rules of procedures, the Delegation Agreement, approved Regional Entity annual compliance enforcement program, annual implementation plans, required program attributes, and the NERC compliance program procedures. These evaluations shall be provided to the appropriate ERO governmental authorities to demonstrate the effectiveness of each regional entity.

<sup>6</sup> See NERC Rules of Procedure at § 1207 ("Regional Entity Audits - Approximately every three years and more frequently if necessary for cause, NERC shall audit each regional entity to verify that the regional entity continues to comply with NERC rules of procedure and the obligations of NERC delegation agreement.").

The Regional Reliability Standards Development Program, Funding, and Event Analysis were areas added to the Regional Entity Audit Program.

The Regional Entity's role in Reliability Assessments was not included in the audit activities as NERC maintains control of and plays an active role throughout this process. NERC's independent reliability assessment is based on constant communication with the eight Regions regarding data collection, self-assessments, and development of reliability assessment reports. In addition, to address emerging reliability considerations, NERC obtains perspectives, data and information from the Regions to fortify its Special Reliability Assessments.

The draft AUPs were sent to each NERC program owner to review accuracy. NERC provided the draft AUPs to the eight Regional Entities and FERC for review and comment. This was done to promote and maintain transparency of the Regional Entity Audit Program. Based on comments received, NERC revised areas of the original audit plan, specifically associated in the area of funding and data security.

## Chapter 3 – Audit Process

### Compliance and Certification Committee Participation

The CCC is a NERC BOT appointed stakeholder committee. The CCC monitors NERC's compliance with the ROP while maintaining independence of the execution of NERC's programs. In meeting its obligation, a CCC member was designated to observe the Regional Entity audit to maintain oversight of NERC's implementation of the Regional Entity Audit Program.

### Pre-Audit

Prior to the audit, NERC sent ReliabilityFirst three requests for information (RFI), Parts 1, 2 and 3, and corresponding questionnaires. RFI Part 1 is focused on CMEP items; RFI Part 2 on the ERO functional responsibilities; and RFI Part 3 is specific to finance and budget.

ReliabilityFirst responded and provided the requested information to NERC within the time specified.

NERC identified the Crowe and NERC audit team members to ReliabilityFirst. NERC provided to ReliabilityFirst each Crowe team member's work history, Confidentiality Agreements and Conflict of Interest statements. The CCC member signed the NERC Conflict of Interest and Confidentiality Agreement statements and provided his work history. These documents were provided to ReliabilityFirst prior to the audit.

NERC, in conjunction with Crowe staff, held a pre-audit conference call on March 3, 2009 with the ReliabilityFirst executive management team and staff. Also participating on the call, was a member of the CCC and FERC. The purpose of the call was to provide all parties involved with an understanding of the audit process and to address questions from ReliabilityFirst.

### On-Site Process

The audit started Monday, March 23, 2009 at 8:00 a.m. EST at ReliabilityFirst's office. At 10:00 a.m., NERC delivered an introduction presentation to the ReliabilityFirst staff. Topics included in the presentation were:

- Introductions of the Crowe and NERC audit team members and observers;
- Scope of the audit;
- Regional Entity audit regulatory references;
- Roles and responsibilities; and
- Deliverables and timelines

### Week One Activities

Crowe staff completed the procedures associated with Notices and Compliance. The ERO, Registrant Reporting, Mitigation Plans, Penalty and Sanctions, and Independence were started and partially complete by the end of the first week.

NERC staff performed an assessment of ReliabilityFirst's Information Systems and details concerning this assessment are contained in Chapter 5, Information Systems, of this report.

Crowe and NERC staff held interviews with key ReliabilityFirst personnel to validate evidence presented. FERC staff was in attendance for the majority of the interviews.

### **Week Two Activities**

Crowe staff completed the remaining procedures started in week one, including starting and completing Registration and Certification procedures. The NERC Regional audit team validated a compliance audit that ReliabilityFirst performed on one of its registered entities. Details concerning NERC validation of the compliance audit are contained in Chapter 6, Compliance Audit Validation, of this report.

### **Status Updates**

A status update occurred with ReliabilityFirst executive and management personnel at approximately 4:30 p.m. each day. Items discussed included the following:

- Completed activities for the day, including a dashboard with the percentage of AUPs completed;
- Planned activities for the following day;
- Interview schedules;
- Open requests for information items;
- Possible exceptions to the AUPs; and
- Possible management letter items.

ReliabilityFirst was given the opportunity to comment and supply additional information for clarification.

### **Exit Presentation**

On April 3, 2009 at 3:30 p.m., an exit presentation was delivered to ReliabilityFirst executive management and staff. Crowe discussed the basis for noted exceptions to the procedures and management letter items. NERC delivered a presentation communicating the results on the areas in which NERC staff performed its assessment (Information Systems and validation of the compliance audit).

### **Audit Information Security and Confidentiality**

All information collected as part of the audit process is contained in electronic format. The electronic evidence was placed in a sealed, tamper-proof envelope verified by NERC staff and stored at a secure location. It will be retained for historical evidence per NERC's data retention policy.

## Chapter 4 – Financial and Budget Management

---

### Background

Pursuant to Section 8 (j), “Funding,”<sup>7</sup> of the “Amended and Restated ReliabilityFirst Regional Delegation Agreement between North American Electric Reliability Corporation,” NERC has the obligation to perform a review of ReliabilityFirst’s financial records, at a minimum of three years. NERC developed audit criteria with Crowe based on the requirements outlined in the Delegation Agreement and in the form of an AUP. The majority of criteria developed included items which an independent financial auditing firm should include in its annual review of the Regional Entity’s financial records. Based on subsequent discussions, it was determined that in lieu of duplicating the efforts of the ReliabilityFirst independent auditing firm, ReliabilityFirst would provide NERC copies of various requested documents, which would affirm to NERC all items necessary for adherence to Section 8, Funding, were met and provided.

### Discussion of Review

ReliabilityFirst contracts a Tier 1 independent accounting firm to perform a financial audit of its books annually and submits its financial audit report to NERC. In addition to ReliabilityFirst’s independent financial audit report, NERC requested additional information, which is represented in the list below.

1. Accounting Policies and Procedures;
2. ReliabilityFirst’s Chart of Accounts;
3. ReliabilityFirst’s Audit Arrangement letter from its independent financial auditing firm;
4. Audit Scope Letter;
5. ReliabilityFirst’s 2008 Quarterly Unaudited Financial Statements and Actual to Budget Variance Analysis;
6. ReliabilityFirst’s 2008 Audited Financial Statements and Independent Auditor’s Report;
7. ReliabilityFirst’s 2009 Business Plan and Budget; and
8. Completed Pre-Audit Questionnaire concerning finance and budget items

### Conclusion

NERC’s Chief Financial Officer (CFO) performed a detailed review of requested documentation supplied by ReliabilityFirst and concluded ReliabilityFirst had complied with its obligations as required by its Delegation Agreement. The CFO’s determination was based on the documentation provided, including reliance upon the independent financial auditor’s report, the independent audit of the financial statements, and no additional correspondence between ReliabilityFirst and its financial auditor was required.

---

<sup>7</sup> See the Executed “Amended and Restated Delegation Agreement between North American Electric Reliability Corporation and ReliabilityFirst Corporation at, §8(j) (“NERC shall have the right to review from time to time, in reasonable intervals but no less than every three years, the financial records of ReliabilityFirst in order to ensure that the documentation fairly represents in all material respects appropriate funding under this Agreement.”)

## Chapter 5 – Information Systems

---

### Discussion of Review

Pursuant to requirements outlined in ROP Section 402.3,<sup>8</sup> NERC staff in conjunction with Crowe staff, developed criteria for assessing the Regional Entities' process for maintenance of data security, confidentiality, and integrity.

The assessment was performed by a Senior Regional Entity Compliance Program Auditor and the Manager of Situation Awareness and Infrastructure Security. The CCC observer was also present. Due to the confidential nature of the information reviewed, this report contains a summary of key areas evaluated.

### Data Security, Access Control, and Confidentiality

ReliabilityFirst has adequate processes and procedures in place for maintenance of data security and confidentiality. Spot checks were conducted to ensure ReliabilityFirst adhered to its process. ReliabilityFirst places strict controls over its confidential data. The NERC audit team validated the controls by performing tests to ensure unauthorized persons could not access the data.

Hard copy files were found to be placed in a secure location with access logging and unauthorized access controls in place. The audit team performed a verification of these controls by attempting access. The audit team concluded ReliabilityFirst's security systems functioned as designed, preventing unauthorized personnel from accessing the documents.

ReliabilityFirst maintains an access list for both electronic and physical data. The authorized list is reviewed annually by a ReliabilityFirst executive. The audit team verified that ReliabilityFirst followed its policy for removing access within the time specified for an employee who was no longer employed by ReliabilityFirst.

### Classification of Data

ReliabilityFirst's procedures for classification of data were reviewed. The audit team selected several samples to verify consistent use of the classification and protection of confidential materials. The audit team concluded ReliabilityFirst adhered to its procedure for classifying data.

### Data Transmittal

ReliabilityFirst has various policies to protect data in transit, including the use of secure electronic sites as needed for data transfer. Multiple barriers are in place to access confidential data, which requires specific authorization.

---

<sup>8</sup> See Rules of Procedure at § 402.3 ("Information Collection and Reporting — NERC and the regional entities shall implement data management procedures that address data reporting requirements, data integrity, data retention, data security, and data confidentiality.").

### **Data Backup and Recovery**

ReliabilityFirst staff performs frequent backups of the data and stores it off-site in a secure location. Both incremental and complete backups are performed on a scheduled basis per ReliabilityFirst's policy. Security access is required to enter the on-site storage of backup material. The audit team validated the list of personnel with access to the backup data storage, including testing to ensure access was limited per the policy.

The audit team determined ReliabilityFirst follows its policy for maintenance of data security at its off-site data storage. No third party contractors are involved. The off-site data storage facility is located remotely from the ReliabilityFirst office as part of ReliabilityFirst's business continuity plan. Access to the facility is strictly controlled and is limited to specified ReliabilityFirst personnel.

### **Data Security Monitoring**

ReliabilityFirst controls access to all areas of its facility. Access rights are determined on a "need to know" basis. The approval of a ReliabilityFirst executive is required prior to authorizing access. All unauthorized access attempts are logged and reviewed by the system administrator.

### **Conclusion**

Upon review of ReliabilityFirst's processes and procedures, the NERC Regional audit team concluded that ReliabilityFirst has robust controls in place for maintaining security of data, and determined this should be considered as a best practice.

## Chapter 6 – Compliance Audit Validation

---

### Discussion of Review

Pursuant to ROP Section 402.1.3.2,<sup>9</sup> NERC, in maintaining its oversight of the Regional Entity Compliance Monitoring and Enforcement Program, must validate the results of a Compliance audit performed by the Regional Entity on one of its registrants. To meet this obligation, NERC validated the results of an audit of a registered entity *ReliabilityFirst* previously performed. The audit team consisted of a Senior Regional Entity Compliance Program Auditor and two Regional Compliance Auditors from NERC. The NERC audit team reviewed the evidence supplied by the registered entity to *ReliabilityFirst*, the associated Reliability Standards Audit Worksheets (RSAWs), and the *ReliabilityFirst* audit report to make its determination.

The audited entity is registered as a Transmission Owner, Distribution Provider, Load Serving Entity and Purchasing-Selling Entity. As such, the audit team performed an assessment of 23 reliability standards that were subject to the audit performed by *ReliabilityFirst*. The NERC Regional audit team verified that *ReliabilityFirst* included all reliability standards applicable to the registered entity per its registration. A representative from FERC staff and the CCC observed portions of the NERC Regional audit validation. Detailed notes by the NERC Regional audit team were taken and captured in the RSAWs submitted by *ReliabilityFirst* as evidence. These will be retained as historical data per NERC's data retention policy.

### Conclusion

Upon review of the evidence presented, the NERC Regional audit team found the conclusions reached by *ReliabilityFirst* to be accurate.

---

<sup>9</sup> See Rules of Procedure at § 402.1.3.2 (“NERC shall establish a program to audit bulk power system owners, operators, and users operating within a regional entity to verify the findings of previous compliance audits conducted by the regional entity to evaluate how well the regional entity compliance enforcement program is meeting its delegated authority and responsibilities.”).

## Appendix A – AUP Exceptions to the Rules of Procedures, Delegation Agreement and Other

---

Note: The exceptions listed in Appendix A were quoted from the Crowe Horwath LLP Report. The notes were added by NERC for clarification.

### **Data Retention and Confidentiality**

*See Crowe report at § II.B.9.a (CMEP 3.1.5)*

“Exception noted. CMEP 3.1.5 requires REs to provide copies of audit team members’ signed Confidentiality or Non-Disclosure Agreements to registered entities prior to a compliance audit. Per inquiry with RFC, during 2008, it was not part of RFC’s process to provide copies of audit team members’ Non-Disclosure Agreements to registered entities. During our procedures, 5 out of 5 items tested did not have a non-disclosure agreement sent to the registered entity.”

*See Crowe report at § II.B.13.a.iv (ROP 1503.7)*

“Exception noted. ROP 1503.7 states that the RE must publicly post any denied requests for confidential information, including an explanation of the reasons for the denial. However, the decision not to disclose confidential information was not posted on the RFC website.”

### **Independence**

*See Crowe report at § III.B.4.b (ROP 403.6.5)*

“Exception noted. ROP 403.6.5 states that an independent consultant working for a regional entity compliance enforcement program cannot have received compensation from a BPS owner, operator, or user within the preceding six months. For one (1) out of six (6) independent consultants, it was noted that both the Work History and Conflict of Interest Questionnaire were not signed. Therefore, we could not confirm whether the contractor had received compensation from a BPS owner, operator or user.”

### **Reporting to NERC**

*See Crowe report at § IV.B.8.a.ii – (CMEP 8.0)*

“Exception noted. CMEP 8.0 requires that violations other than those that require 48-hour notification must be reported to NERC within 5 business days of the RE’s determination that an alleged violation may have occurred. This procedure was applicable to 6 violations. Of those 6 violations, 5 were not reported to NERC within the 5 day period.”

*See Crowe report at § IV.B.12.c.i.a – (CMEP 6.5)*

“Exception noted. CMEP 6.5 requires that the RE notify NERC within 5 business days of accepting a mitigation plan. However, for 1 out of the 10 sampled items to which this procedure applied, the date on the RFC’s transmittal of notification and mitigation plan to NERC did not occur within 5 business days of the date the RE accepted the mitigation plan.”

## Compliance

See Crowe report at § VII.A.4.a.i – (ROP 403.7.5; CMEP 3.1.5; Compliance Auditor Manual, section 6)

“Exception noted. ROP 403.7.5 and CMEP 3.1.5 require that compliance audit participants complete required auditor training prior to the start of the audit. For one audit out of 5, one team member took the online Gathering Quality Evidence training on 9/16/08, which was not prior to the start of the compliance audit on 9/15/08.”

See Crowe report at § VII.A.4.e.iii.a.i – (CMEP 3.1.1)

“Exception noted. Per CMEP 3.1.1, the RE must provide a registered entity with the employment history of original audit team members at least 2 months prior to the commencement of the on-site audit. However, in Audit No. 5, RFC did not supply the work history for one of the original scheduled audit team members until 13 days before the onsite audit. This team member was listed in RFC’s notification letter to the audited registered entity, but was not listed in the staff work history letter that RFC sent to the registered entity 60 days before the audit. No other exceptions were noted.”

See Crowe report at § VII.A.4.g.i – (CMEP 3.1.1)

“Exception noted. CMEP 3.1.1 states that the RE is to provide audit materials to compliance audit participants. “Compliance audit participants” are the audited registered entity and the audit team members. We obtained documentation that RFC provided the audit materials to registered entities in 5 of 5 audits without exception. However, RFC could not provide evidence that they provided audit materials to the members of the audit team in 5 of 5 audits. RFC stated that members of the audit teams have access to audit materials such as the RSAWs on RFC's internal shared compliance drive or via a secure internet site.”

See Crowe report at § VII.A.4.n.iii.k).iii – (ROP Compliance Auditor Manual, section 12.3, NERC Compliance Audit Report Template)

“Exceptions noted. CMEP 3.1 states, “All Compliance Audits shall be conducted in accordance with audit guides established for the Reliability Standards included in the Compliance Audit.” Section 12.3 of the Compliance Auditor Manual states that audit reports are to include information on supervisory reviews obtained. This is also included in the NERC audit report template. However, for 3 of the 5 audits, the reports did not mention supervisory reviews. We obtained evidence that a supervisor reviewed the audit reports, but this was not documented in the reports themselves. RFC told us that they understood the Compliance Auditor Manual to be a guideline and not a requirement.”

See Crowe report at § VII.A.4.n.iii.k).iv – (Compliance Auditor Manual, section 12.3, NERC Compliance Audit Report Template)

“Exceptions noted. CMEP 3.1 states, “All Compliance Audits shall be conducted in accordance with audit guides established for the Reliability Standards included in the Compliance Audit.” Section 12.3 of the Compliance Auditor Manual states that audit reports are to include a description of the work the RE performed to determine if information obtained was sufficient and appropriate. This is also included in the NERC audit report template. However, for 2 of the 5 audits, the reports did not include a description of work RFC performed to determine if information obtained was sufficient and appropriate (i.e., “appropriateness assessment”).

RFC told us that they understood the Compliance Auditor Manual to be a guideline and not a requirement.”

See Crowe report at § VII.B.1.a.iii.b) – (CMEP 3.3.1)

“Exceptions noted. For the 10 spot checks in our sample, RFC had no documentation as to when they provided the registered entity with an opportunity to comment on the draft assessment. RFC officials told us that they held conversations with the registered entities on the results of their assessments, but these conversations were not documented.”

### **Registered Entity Reporting**

See Crowe report at § VIII.A.3.e. – (CMEP 3.2.1)

“Exception noted. Per the CPI's Senior Engineer, he looks over the weekly compliance report that lists self-certification registrants. He reviews in more detail registrants listed as "not compliant". However, there is no formally documented review of the self-certifications. As a result, there is not a way to verify that the self-certifications were reviewed.”

**Note:** Crowe could not determine performance of items VIII C.3.a.v., C.3.a.vi, and C.3.a.vii. NERC, in its role of subject matter expert, determined ReliabilityFirst had performed an assessment of the Periodic Data Submittals.

See Crowe report at § VIII.C.3.a.v – (CMEP 3.6.1)

“Exception noted. RFC does not formally document its review of certain Periodic Data Submittals. Per the CPI Manager and Senior Engineer, RFC tests that the information received is compliant and follows-up with registrants regarding non-compliant issues through resolution. However, because this review is not documented, there is not a way to verify that it took place.”

See Crowe report at § VIII.C.3.a.vi– (CMEP 3.6.1)

“Exception noted. RFC does not formally document its draft assessments of Periodic Data Submittals. Per the CPI Manager and Senior Engineer, RFC tests that the information received is compliant and follows-up with registrants regarding non-compliant issues through resolution. However, because the draft assessment is not documented, there is not a way to verify that it was made.”

See Crowe report at § VIII.C.3.a.vii – (CMEP 3.6.1)

“Exception noted. RFC does not formally document its final assessments on Periodic Data Submittals. Per the CPI Manager and Senior Engineer, RFC tests that the information received is compliant and follows-up with registrants regarding non-compliant issues through resolution. However, because the final assessment is not documented, there is not a way to verify that it was made.”

## **Investigations**

*See Crowe report at § IX.A.2.d.i – (ROP 403.7.5; NERC Compliance Violation Investigation Process, July 2008, p.6.)*

“Exception noted. ROP 403.7.5 requires that CVI team members complete NERC auditor training prior to performing activities related to the CVI. However, for one of two CVI’s tested, it was not documented whether one CVI Team Member had completed the NERC Auditor training before the performance of CVI Activities.”

## **Penalties, Sanctions, and Settlements**

*See Crowe report at § XI.B.2.a.iv.j – (NERC Settlement Template)*

“Per the NERC Settlement Template, a settlement agreement should include a deadline for paying the penalty settled upon. However, the two applicable settlements did not include a deadline for payment. Exception noted.”

## **Mitigation Plans**

*See Crowe Horwath report at § XII.A.4*

“In 2008, RFC reviewed mitigation plans for completeness and sufficiency. If needed, RFC would request clarification or supporting information to better understand a mitigation plan. RFC would accept a mitigation plan that was sufficiently complete such that it could submit it to NERC. In 2008, RFC had numerous mitigation plan submissions which it reviewed for clarity and completeness. However, it did not have formally documented review documentation (per the "NERC Mitigation Plan Approval Criteria") of the mitigation plans it actually "accepted" and forwarded to NERC through the Workbook. Exception noted.”

*See Crowe Horwath report at § XII.D – (March 18, 2008 Guidance on Mitigation Plans)*

“RFC did not perform the analysis described in the March 18, 2008 Guidance on Mitigation Plans directive from NERC's Chief Executive Officer. RFC does track the progress of the mitigation plans. Exception noted.”

## **ERO Functional Requirements**

### **RFC Standards Process**

*See Crowe Horwath report at § XIII.C.1.b.ii.e.v – RFC Standards Process exception*

“Exception noted. RFC's standards process calls for the appointment of an interim chair of the Standards Drafting Team (SDT) after the SDT has been assembled. For SAR of the we tested, there was no documentation provided that an interim chair was appointed.”

*See Crowe Horwath report at § XIII.C.1.b.vi– RFC Standards Process exception*

“Exception noted. RFC’s Regional Standards Development Process in its Delegation Agreement calls for the SC to set a preliminary date for the SDT to have a draft Standard available. For BAL-502-RFC-02, the documentation of this was not provided. The date was decided at a Board meeting. At the Board meeting, it was indicated the standard would be ready for voting by the end of the year 2008. For EOP-001-RFC-01 and EOP-5001-RFC-01, no exceptions noted.”

*See* Crowe Horwath report at § XIII.C.1.d.ii– RFC Standards Process exception

“RFC’s Standards Development Process in its Delegation Agreement calls for the draft Standard work product to include an assessment of the impact of the SAR on neighboring regions. For BAL-502-RFC-02, an assessment of the impact on neighboring regions was not formally documented in the work product of the Standards Development Team. Exception noted.”

## Appendix B – AUP Exceptions

Note: The exceptions listed in Appendix B were quoted from the Crowe Horwath Report. The notes were added by NERC for clarification.

### **Data Retention and Confidentiality**

See Crowe Horwath report at § II.B.5.b

“Exception noted. The Organization Registration Policy document does not reference critical energy infrastructure information. The Organization Certification Policy does address critical energy infrastructure information.”

### **Independence**

**Note:** There are two distinct sections of Independence AUP which addresses governance and conflict of interest. One area is internal, i.e., ReliabilityFirst staff and board members (Internal Regional Entity (RE) Governance and Conflict of Interest). The other area is relevant to personnel such as contractors (Conflict of Interest by External Parties). As a result, it is noted as two exceptions which pertain to the same criteria.

### **Internal Regional Entity (RE) Governance and Conflict of Interest**

See Crowe Horwath report at § III.A.4.a.iv

“Exception noted. RFC’s written policies do not address reviews of conflict of interest statements or disclosures. There was no documentary evidence available to confirm that the COI statements and Disclosures were reviewed by RFC.” However, RFC officials told us these reviews are performed in practice.”

See Crowe Horwath report at § III.A.4.a.v

“Exception noted. RFC’s Governance Guidelines refer to the recusal of Directors in cases of conflicts of interest. Recusal is not specifically referenced for other individuals.”

See Crowe Horwath report at § III.A.4.a.vii

“Exception noted. Enforcement is addressed in RFC’s conflict of interest policies. However, the monitoring of compliance with conflict of interest policies is not addressed.

“RFC management stated that monitoring procedures were performed. However, there was no documentary evidence to support the performance of monitoring procedures related to Board members, executives and employees.”

### **Conflict of Interest by External Parties**

See Crowe Horwath report at § III.B.2.d

“Exception noted. RFC’s written policies apply to both internal and external parties. As noted in the result to step III.A.4.a.iv above, these policies do not address the reviews of conflict of interest statements or disclosures. However, RFC officials told us these reviews are performed in practice.”

*See Crowe Horwath report at § III.B.2.e*

“Exception noted. RFC’s written policies apply to both internal and external parties. As noted in the result of step III.A.4.a.vii, enforcement is addressed in RFC’s conflict of interest policies. However, monitoring of compliance with conflict of interest policies is not addressed.”

## **Registration**

**Note:** Similar to the Note pertaining to Independence, the following four exceptions (V.A. 6, 8, 10, and 12) are based on the same criteria but applied to different registration criteria and are located in separate steps within the Registration AUP.

*See Crowe Horwath report at § V.A.6*

“We haphazardly selected 3 LSE’s from RFC’s compliance registry and requested documentation that RFC verified that each LSE met one of the criteria noted. Per discussion with the Compliance Manager and Senior Compliance Engineer, there is no formal documentation to show that an LSE met the necessary criteria. They stated that they rely on the entity to register for the necessary functions, and the Senior Compliance Engineer will approve the entity during the registration process. They also rely on compliance audits to determine if an entity is registered for the proper function. Therefore, RFC verifies an entity meets the criteria for a function, but there is no formal documentation as to which criteria are met and how they are met. Exception noted.”

*See Crowe Horwath report at § V.A.8*

“We haphazardly selected 3 DP’s from RFC’s compliance registry and requested documentation that RFC verified that each DP met one of the criteria noted. Per discussion with the Compliance Manager and Senior Compliance Engineer, there is no formal documentation to show that a DP met the necessary criteria. They stated that they rely on the entity to register for the necessary functions, and the Senior Compliance Engineer will approve the entity during the registration process. They also rely on compliance audits to determine if an entity is registered for the proper function. Therefore, RFC verifies an entity meets the criteria for a function, but there is no formal documentation as to which criteria are met and how they are met. Exception noted.”

*See Crowe Horwath report at § V.A.10*

“We haphazardly selected 3 GO’s from RFC’s compliance registry and requested documentation that RFC verified that each GO met one of the criteria noted. Per discussion with the Compliance Manager and Senior Compliance Engineer, there is no formal documentation to show that a GO met the necessary criteria. They stated that they rely on the entity to register for the necessary functions, and the Senior Compliance Engineer will approve the entity during the registration process. They also rely on compliance audits to determine if an entity is registered for the proper function. Therefore, RFC verifies an entity meets the criteria for a function, but there is no formal documentation as to which criteria are met and how they are met. Exception noted.”

See Crowe Horwath report at § V.A.12

“We haphazardly selected 3 TOP’s from RFC’s compliance registry and requested documentation that RFC verified that each TOP met one of the criteria noted. Per discussion with the Compliance Manager and Senior Compliance Engineer, there is no formal documentation to show that a TOP met the necessary criteria. They stated that they rely on the entity to register for the necessary functions, and the Senior Compliance Engineer will approve the entity during the registration process. They also rely on compliance audits to determine if an entity is registered for the proper function. Therefore, RFC verifies an entity meets the criteria for a function, but there is no formal documentation as to which criteria are met and how they are met. Exception noted.”

See Crowe Horwath report at § V.B

“Exception noted. RFC has a policy that states, “NERC and Reliability First have the obligation to identify and register all entities that meet the criteria for inclusion in the compliance registry if an entity elects not to self register.” However, RFC does not have written procedures for assuring that this is done.”

See Crowe Horwath report at § V.C.1.b

“Exception noted. This verification is not documented during the registration process.”

Note: §V.C.1.b relates to evidence that the Regional Entity checked that the relevant area was under only 1 Reliability Coordinator.

See Crowe Horwath report at § V.C.1.c

“Exception noted. This verification is not documented during the registration process.”

Note: §V.C.1.c relates to evidence that the Regional Entity checked that each registered transmission element in its region was under only 1 Transmission Planner, Planning Authority, and Transmission Operator.

See Crowe Horwath report at § V.C.1.d

“Exception noted. This verification is not documented during the registration process.”

Note: §V.C.1.d relates to the Regional Entity checking that each registered load and generator in their Region are only under 1 Balancing Authority.

## **Compliance**

See Crowe report at § VII.A.4.i.

“Exception noted...Section 9.2 of the Compliance Auditor Manual states that regional entities are to use the Reliability Standards Audit Worksheets (RSAWs) to document their review and assessment of compliance with reliability standards during compliance audits.

- “For Audit No. 2 in our sample, 1 of the 10 RSAWs we reviewed did not include any of the checklist items from the NERC standard RSAW. RFC told us that they understood the Compliance Auditor Manual to be a guideline and not a requirement.”

- “For 5 of the 5 audits in our sample, none of the RSAW checklist items were marked as complete. RFC told us that they understood the Compliance Auditor Manual to be a guideline and not a requirement.”
- “For Audit No. 2 in our sample, 5 of the 10 RSAWs we reviewed did not include statements of compliance with the requirements in the RSAWs. RFC told us that they understood the Compliance Auditor Manual to be a guideline and not a requirement.”
- “For one compliance audit out of 5 compliance audits tested, 2 of the 10 RSAWs did not include supporting documentation or a description of the documentation that was reviewed for one or more requirements. RFC told us that they understood the Compliance Auditor Manual to be a guideline and not a requirement.”

*See Crowe Horwath report at § VII.A.4.n.i*

“Exceptions noted. For 2 of 5 audits, no documentation was provided to demonstrate that the final audit report was provided to the registered entity.”

*See Crowe Horwath report at § VII.A.4.o.iii*

“Exception noted. On 1 of the 10 RSAWs we inspected for 1 of 5 compliance audits, we found one requirement on an RSAW that was marked "Possible Violation." According to the audit report, this item was determined not to be a violation. This item was also not listed as a possible violation in the exit briefing presentation that was given the last day the audit team was onsite. The audit team lead stated that they had obtained appropriate documentation to eliminate this finding before the audit was concluded. However, the RSAW was not revised to reflect this.”

## **Investigations**

*See Crowe Horwath report at § IX.A.1*

“Exception noted. RFC does not have written procedures for initiating compliance violation investigations.”

*See Crowe Horwath report at § IX.A.2.c*

“RFC did not provide documentation to support the decision to initiate the CVI. Exception noted.”

## **Mitigation Plans**

*See Crowe Horwath report at § XII.A.5*

“Exception noted. We noted 3 of 10 examples where RFC did not send the registrant a written notice accepting or rejecting the mitigation plan.”

## **ERO Functional Requirements**

*See Crowe Horwath report at § XIII.B.2.a.iv*

“For 1 event analysis of 6, RFC did not provide documentation of when the event analysis was initiated. Exception noted.”

## Appendix C – AUP Procedures List

---

### Implementation Plan:

(Section 4 CMEP, ROP 403.8, ROP 403.9, and ROP 403.21)

### Data Retention and Confidentiality

(Section 9 CMEP, ROP 402.8, ROP 403.6.4, ROP 403.7.4, ROP 403.14, ROP 403.16, ROP 408.3.1, ROP 502.2.1, and ROP 502.2.2)

### Independence [Organizational Independence and Conflict of Interest]

(ROP 402.8, ROP 403.1, ROP 403.6.1, ROP 403.6.2, ROP 403.6.3, ROP 403.6.5, ROP 403.7.1, ROP 403.7.2, and ROP 403.7.3)

### Information Systems

(ROP 402.3)

### Reporting to NERC

(Section 8 CMEP, ROP 401.3, ROP 403.10, ROP 403.15, ROP 403.19, ROP 403.20, ROP 403.21.1, ROP 408.1, ROP 408.2, ROP 408.4, ROP 410.3, ROP 502.1.4, ROP 502.1.5, ROP 503.3.3.3, ROP 503.3.3.4, ROP 504.2, ROP 507.4, ROP 507.6, and throughout the CMEP sections)

### Registration

(Section 2 CMEP, ROP 500 and Appendix 5)

### Certification

(Section 2 CMEP, ROP 500, and Appendix 5)

### Compliance (Audits and Spot Checks)

(Section 3.1 CMEP, ROP 403.7.5, & ROP 403.11; Section 3.3 CMEP, and ROP 403.10.6)

### Registered Entity Reporting (Self-Certifications, Exception Reporting, Self-Reporting, Periodic Data Submittals)

(Section 3.2 CMEP, Section 3.7 CMEP, Section 3.5 and CMEP, Section 3.6)

### Investigations (Compliance Violation Investigations, Complaints)

Section 3.4 CMEP, and ROP 403.13, (Section 3.8 CMEP)

### Notices (Possible, Alleged and Notices of Confirmed or Dismissals)

(Section 5.1 CMEP)

### Penalties and Sanctions

(ROP 403.17, ROP 407.2, and Appendix 4B)

### Mitigation plans

(ROP 403.18, and Section 6 CMEP)

### Remedial actions

(Section 7 CMEP)

### Hearings

(ROP 403.4, ROP 403.20, and ROP 407.3, Attachment 2 to the CMEP)

### ERO Functional Requirements (Regional Delegation Agreements)