# Table of Contents

Preface .......................................................................................................................... iii  
Executive Summary ....................................................................................................... iv  
Introduction .................................................................................................................... v  
  Purpose ......................................................................................................................... v  
  Background ................................................................................................................... v  
  Current data retention approach ............................................................................... v  
Chapter 1 – Methodology .............................................................................................. 1  
  Current data retention requirements and guidance .................................................... 1  
  Responses from industry to the Data Retention Survey ............................................ 2  
Chapter 2 – Results ....................................................................................................... 3  
  Current data retention requirements and guidance .................................................... 3  
  Responses from industry to the Data Retention Survey ............................................ 3  
  Overview ..................................................................................................................... 3  
    Registered entity concerns with current data retention policies ............................ 4  
    Registered entity concerns with current RSAWs .................................................... 4  
Chapter 3 – Recommendations .................................................................................... 6  
  Standard Development ............................................................................................... 6  
  Auditor data sampling ............................................................................................... 6  
  RSAW Improvements ............................................................................................... 8  
  Compliance communication tools redesign .............................................................. 8  
  Required next steps ................................................................................................... 9  
Chapter 4 – Conclusion ................................................................................................ 10  
Appendix 1 – Frequently Asked Questions  
Appendix 2 – References  
Appendix 3 – NERC Reliability Standards data retention requirements  
Appendix 4 – GAGAS references  
Appendix 5 – Rules of Procedure references  
Appendix 6 – Data Retention Survey Results  
Appendix 7 – Common data types
Preface

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to ensure the reliability of the bulk power system (BPS)\(^1\) in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC’s area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the electric reliability organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC’s jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

The North American BPS is divided into several assessment areas within the eight Regional Entity boundaries, as shown in the map and corresponding table below.

| FRCC | Florida Reliability Coordinating Council |
| MRO | Midwest Reliability Organization |
| NPCC | Northeast Power Coordinating Council |
| RF | ReliabilityFirst |
| SERC | SERC Reliability Corporation |
| SPP-RE | Southwest Power Pool Regional Entity |
| TRE | Texas Reliability Entity |
| WECC | Western Electricity Coordinating Council |

As has been presented in the concept papers for the Reliability Assurance Initiative (RAI), NERC and the Regional Entities (known collectively as the ERO Enterprise) are moving to a risk-based strategy, particularly in the areas of Compliance and Enforcement. At the start of 2013, the ERO Enterprise assembled an advisory group to provide input and advice for modification of existing NERC Reliability Standard data retention requirements. The data retention team is comprised of representatives from NERC and the NERC Compliance and Certification Committee (CCC).

Beginning in 2013, the data retention team began reviewing and analyzing current data retention requirements and soliciting industry feedback on current data retention requirements. This white paper presents the information reviewed by the team and makes recommendations for changes to current guidance documents, future NERC Reliability Standard development, and auditing processes.

---

1 Pursuant to the Energy Policy Act of 2005, NERC and FERC have jurisdiction over users, owners, and operators of the BPS. Section 215 of the Federal Power Act defines BPS as the facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof) and electric energy from generation facilities needed to maintain transmission system reliability. FERC has recognized that users, owners, and operators of the BPS are users, owners and operators of the Bulk Electric System (BES). The definition of BES went into effect July 1, 2014. See NERC Glossary of Terms available at: http://www.nerc.com/files/glossary_of_terms.pdf. See also, 146 FERC ¶ 61,199, March 20, 2014). Nothing in this document limits the jurisdictional authority of NERC and FERC pursuant to the Energy Policy Act of 2005 and Section 215 of the FPA.
Executive Summary

This white paper is a product of the data retention team’s analysis and explores possible options for establishing uniform tools and applications and standardizing evidence retention requirements across the ERO Enterprise to promote consistency in demonstrating compliance. These options should provide improvements that support reliability and ensure that resources allocated by the ERO Enterprise and registered entities are commensurate with the potential risks of noncompliance to reliability. This white paper recommends that NERC modify data retention requirements so that the burden of producing records necessary to demonstrate compliance is commensurate with the risk to the reliability of the BPS.

The data retention team also recommends including in new Reliability Standards a consistent data retention period of either a rolling 6-months for high-volume data, or a 4-year retention period for all other data, with two specific exceptions: 1) Standards requiring a current program or procedure, which would be limited to the currently effective version with a revision history specifying changes and dates of review; and 2) Standards requiring testing at intervals, which would require the retention of the last full testing record and evidence of recurrence. In addition, this white paper recommends simplifying data requests by including as a part of the ERO Compliance Auditor Manual and Handbook a recommendation that, regardless of the data retention requirements of the Standard and time between Compliance Audits, auditors focus sampling to the most recent two years. This recommended method of sampling would be more efficient and less burdensome for registered entities and the ERO Enterprise. By instituting the recommended method of sampling, the ERO Enterprise and registered entities could reallocate resources to areas of greater risk to the reliability of the BPS.

Feedback on the recommendations outlined in this white paper will focus and refine the ultimate data retention requirements and auditor sampling methodology.

---

2 “High-volume data,” as used herein, refers to electronic data sets and files, paper documents, or audio recordings with sizes making it cost- or space-prohibitive to gather, maintain, track, and provide the data to auditors within a reasonable period. Examples of high-volume data could be access logs, video surveillance tapes, or voice and telephone recordings.

3 For example, PRC-005 requires a registered entity to provide evidence that its distinct maintenance activities have been performed within the intervals identified by the registered entity in its Protection System Maintenance Program.
Introduction

Purpose

The ERO Enterprise assembled a working team to assess the data retention requirements of the NERC Reliability Standards, Rules of Procedure, and the current guidance on data requests to registered entities. The goal of this effort was to determine the burdens of document retention and compliance data requests in order to balance those factors with potential risk of noncompliance to the reliability of the BPS.

The purpose of this white paper is to provide background and technical rationale for proposed revisions to the data retention requirements in new and revised NERC Reliability Standards and to the methodology of Compliance Audit and Spot Check data sampling requests. The goal is to minimize the Compliance Enforcement Authority (CEA) and registered entity resources used for gathering, storing, and producing data while maintaining reasonable assurance of compliance with the effective NERC Reliability Standards and reliability of the BPS.

The data retention team:

- Identified and evaluated current data retention requirements;
- Recommended improvements to reduce the data-maintenance burdens on registered entities;
- Provided guidance regarding the levels of data necessary to support proof of compliance;
- Recommended revised data retention requirements to be commensurate with risk to the BPS; and
- Recommended methods of sampling that are more efficient and less burdensome for registered entities.

There is no current consistent data retention period prescribed by the Commission or NERC applicable to all Reliability Standards. There are different requirements for the length of time registered entities must keep identical types of data for certain Reliability Standards. The ERO Enterprise has considerable flexibility to determine and identify how long a registered entity must retain evidence to show compliance. This flexibility allows the ERO Enterprise to consider altering data retention requirements and data sampling methodologies.

This document describes current retention requirements for data sampling techniques and provides justification for, and proposes guidance on, data retention requirements within the NERC Reliability Standards and requirements, both through the standards review process for existing Standards and through standards development for future Standards.

Background

In November 2012, the ERO Enterprise began to develop the RAI, a multi-year effort to identify and implement changes that enhance the effectiveness of the Compliance Monitoring and Enforcement Program (CMEP). The experience of the past several years demonstrates that it is not practical, effective, or sustainable for the ERO Enterprise to monitor and control all compliance to the same degree and to treat all noncompliance with the same level of process and evidentiary requirements.

RAI is the ERO Enterprise’s strategic initiative to transform the current compliance and enforcement program into one that is forward-looking, focuses on high reliability risk areas, and reduces undue administrative burden on registered entities. The goal of RAI is to implement a risk-based program for compliance monitoring and enforcement of Reliability Standards, which provides reasonable assurance through compliance monitoring, applies appropriate discretion in enforcement, and ensures a feedback loop for the improvement of Reliability Standards.

Current data retention approach

At the beginning of NERC’s CMEP, the ERO Enterprise took a prescriptive approach to data retention. Each registered entity was required to have historical documents for the entire audit period as evidence of compliance for each applicable measure included in a Reliability Standard.
Each registered entity is required to provide to NERC and its applicable Regional Entity information necessary to monitor compliance with the NERC Reliability Standards. Each Compliance Audit includes a review of supporting documentation and evidence used by the registered entity. Each CEA has the authority to collect the necessary information to determine compliance and develop processes for gathering data from the BPS owners, operators, and users it monitors.

The NERC Rules of Procedure and the NERC Reliability Standards describe the retention periods for information. The audit review period is typically every three or six years, depending upon the functional registration of the registered entity. In addition, registered entities must retain and provide historical documents for investigations resulting from complaints or events. Certain NERC Reliability Standards contain specific provisions relating to document retention. In some cases, the document retention period is less than the three- or six-year audit period because there would be an “undue burden due to the volume of the data or information required.” In other instances, the NERC Reliability Standards require retention only of the current, in-force version of a policy, plan procedure, or other singular document.

---


5 NERC Standards Process Manual at 6 (Sept. 2010) (stating that there is to be a section in each Standard for Evidence Retention).

6 NERC Bulletin on Data Retention Requirements at 1 (May 20, 2011). For example, NERC recognizes that retaining three-second data from an Energy Management System (EMS) or a Supervisory Control and Data Acquisition (SCADA) system for every three or six years would pose an undue burden due to the volume of records to be retained. In such cases, the audit team will look to the NERC Reliability Standard for guidance regarding a reasonable data retention period.

Chapter 1 – Methodology

Current data retention requirements and guidance

Beginning in 2013, the data retention team conducted a review of current in-force documents, processes, and procedures to determine the full scope of data retention requirements. The data retention team began reviewing and analyzing the data retention requirements in all currently-enforceable and NERC Board of Trustee approved NERC Reliability Standards, the NERC Rules of Procedure, and guidelines for auditing included in the Generally Accepted Government Auditing Standards (GAGAS). Finally, the data retention team reviewed the ERO Enterprise Compliance Auditor Manual and Handbook (Auditor Manual).

Section 215 of the Federal Power Act requires the ERO to develop mandatory and enforceable reliability standards, which are subject to Commission review and approval. The data retention team reviewed both Commission-approved standards and standards adopted by the NERC Board of Trustees. The team reviewed 136 standards, each including multiple requirements, within the 14 families of NERC Reliability Standards. Each requirement was analyzed to determine the: 1) enforcement date; 2) the currently prescribed data retention period; 3) the Violation Risk Factor (VRF); and 4) the Violation Time Horizon. A table covering these factors is included as Appendix 3. Each of the above-listed factors were considered by the data retention team in determining what an appropriate but consolidated and efficient data retention period may be for each kind of evidence. The team then compared the types of evidence required to determine compliance by standard to identify any existing consistencies and the type of data with the risk posed by a violation of the Standard. These determinations formed the basis of the recommended data retention periods, which were then included with a survey to representatives from registered entities to confirm whether these periods would be technically supportable.

Relevant auditor guidance is located within the following documents: 1) ERO Enterprise Compliance Auditor Manual; 2) Compliance Auditor Role Expectations Guide; 3) GAGAS; 4) Institute of Internal Auditors International Professional Practices Framework (IIAIPPF); 5) Public Company Accounting Oversight; and 6) NERC’s Rules of Procedure including Appendix 4C NERC Compliance Monitoring and Enforcement Program (CMEP) Sec. 3.1. The full listing of references within GAGAS for reviewing evidence is included in Appendix 4. The Manual currently consists of three primary parts: the Handbook, the Checklist, and the Glossary of Terms. Additional revisions under development include a section on sampling methodology.

As various RAI projects have evolved, the data retention team continued to evaluate if any programs, projects, or pilots either influenced its recommendations for retention, or could be affected by the recommendations of the team.

---

10 The data retention team did not review standards still in development, although recommendations from this white paper will be forwarded to Standard Drafting Teams for future use.
Responses from industry to the Data Retention Survey

On December 4, 2013, the team sent a data retention survey to CCC representatives. The survey focused on industry experience and feedback on data retention requirements and Reliability Standard Audit Worksheets (RSAWs).

The team received 155 unique individual responses representing nearly 700 registered functions. The full results and responses to the Data Retention Survey are included in Appendix 6. The data retention team reviewed the responses to support the recommendations outlined within this white paper and to determine how registered entities are affected by current data retention requirements. This effort should allow the ERO Enterprise to focus its efforts on those areas presenting the greatest burden to registered entities, without introducing risk to the reliability of the BPS.
Chapter 2 – Results

Current data retention requirements and guidance

The only mandatory and enforceable components of a Reliability Standard are the: 1) applicability; 2) requirements; and the 3) effective dates. Any additional items are included in the Reliability Standard for informational purposes, to establish the relevant scope and technical paradigm, and to provide guidance to registered entities concerning how the CEA will assess compliance.

The NERC Reliability Standards do not have a consistent approach to evidence retention—different retention periods apply to various requirements and data types. For example, BAL-001-0.1a requires a one-year retention period for real-time operating data and VAR-002-2b requires two years of real-time operating data. COM-001-1.1 requires a 90-day retention of operator logs. According to IRO-006-5, if the records are audio recordings, they have a 90-day retention but if documented transcripts then it should be 12 months. MOD-028-2 requires retaining data for 12 months for seven of its requirements, but either 14, 30, or 60 days for two other requirements.\(^{11}\)

There are no specific references in any relevant auditor guidance as to how much data or what age of data to review to confirm compliance. The Auditor Manual does not contain any size-related requirements for sampling data. In fact, the Auditor Manual has included in its Action Item Tips & Techniques section that “[a]vailable evidence may be limited by data retention requirements of the Reliability Standard or NERC guidance.” According to GAGAS, it is the auditor’s professional judgment as to whether evidence is sufficient to address the audit objectives.\(^{12}\)

As with the other current references to data retention, the Rules of Procedure also do not include any guidance on specific retention periods for registered entities. The NERC Rules of Procedure do reference amounts of time for either Regional Entity or NERC retention. The full listing of references within the NERC Rules of Procedure for reviewing evidence is included in Appendix 5. The Rules of Procedure leave the assignment of data retention and reporting requirements to NERC or the Regional Entity.\(^{13}\)

Responses from industry to the Data Retention Survey

Respondents to the Data Retention Survey included representatives from 135 distinct entities including Independent System Operators, small cooperatives, city utilities, dispersed power generators, and trades associations. The majority of registered entity industry respondents were on a six-year audit cycle. In addition, the survey responses indicated that almost 80% of the registered entities had a data retention policy that covered all data retention obligations and had a data historian for archiving time-based data (e.g., SCADA).

Overview

The survey feedback, for the most part, confirmed the industry’s interest in BPS reliability. The responses had the common recommendation that whatever the changes may end up being, they should be simple, intuitive, standardized, and focused on reliability. The responses voiced a frustration and opinion that the focus of auditor data requests and NERC Reliability Standards data retention requirements are on proving compliance and not enhancing reliability. In addition, commenters remarked that data requirements should be more accordant with RAI and should be moving away from zero tolerance issues and towards a focus on internal processes and continuous improvement.

\(^{11}\) The full listing of current and pending NERC Reliability Standards with summarized data retention requirements is included in Appendix 3.

\(^{12}\) The full listing of references within GAGAS for reviewing evidence is included in Appendix 4.

\(^{13}\) See NERC Rules of Procedure at Section 401.3, P22.
Registered entity concerns with current data retention policies

The survey results listed the following three most challenging or problematic issues with regard to data retention for compliance:

- The differing retention periods between the Standards.
- Requests at Compliance Audits and Spot Checks for data that is no longer relevant.
- The volume of data that entities are required to retain and provide.

Nearly all of the responses supported modifications to the current data retention policies. Those that preferred to stay with the status quo did so out of a concern that changes would require additional financial and staffing resources, not because the current requirements are the best option.

One commenter reported that its Regional Entity tells them to save everything between audits even though the Standards lay out different retention requirements. Another comment stated that auditors told the entity to save data after an audit, but then was never contacted about how long to keep that data. Some entities stated that auditors had requested data outside of the retention periods stated in the Standards. For example, the Standard requires keeping records of "system events related to cyber security" for 90 days but then an auditor expected the entity to keep those records for three years.

A common theme was the belief that any changes need to be forward-looking and considered in a reliability context. Registered entities voiced a desire to focus on current practices and policies instead of historical documents, which may not have been relevant for several years. One commenter presented the example that if there are data gaps five years in the past, these are likely to be significantly less relevant to reliability concerns if all data is subsequently up-to-date and continues to be collected going forward.

Similarly, gaps in administrative documents such as missing signatures may be irrelevant to current risk to reliability, if the current supporting documents are complete. Industry responses did recommend exceptions for data and documents related to events and compliance investigations.

Registered entity concerns with current RSAWs

As Reliability Standard Audit Worksheets (RSAWs) are the primary mechanism to collect data for audits, compliance contacts were surveyed on their observations and experiences with RSAWs. Outlined below is a distillation of the survey comments:

- The most predominant comment was that the RSAWs differed from the Reliability Standard, that the questions asked did not always line up with the Standard, or that the questions were not the most precise way to demonstrate compliance.
- Several respondents noted differences among Regions and auditors in the use and expectations of RSAWs and data format.
- Several respondents felt NERC should provide examples of acceptable evidence (not the only way to demonstrate compliance, but acceptable ways).
- RSAWs could be simpler and easier to fill out.
- CIP data requests for audits differ from what the RSAW contains. The Registered Entity often finds out after data submission that data is preferred in a different format.
- There is not a simple way to flag those things not applicable to the Registered Entity and capture that information for future audits and self-certifications.
- RSAW changes make it difficult to keep up.
• There should be a mechanism to attest to compliance directly in the RSAW for those things that occur infrequently or by exception.

• RSAWs should be developed along with the Reliability Standard and receive industry input.

• Additional data requests during an audit point to a problem with the RSAW, these additional data requests should be tracked to provide feedback to the RSAW improvement process.

• There are redundant questions in RSAWs.

The CCC has a separate RAI team working on suggested RSAW improvements. The raw survey comments were provided to this team.
Chapter 3 – Recommendations

The data retention team is targeting the recommendations contained in this section to the ERO Enterprise and auditing staff. The team does not intend these recommendations to instruct, pressure, or influence a registered entity to alter its preexisting document retention policies. Registered entities are often required to meet several different requirements for data retention. In addition to NERC Standard compliance, entities may be responsible to the Securities and Exchange Commission (SEC) or FERC. Entities may save certain data for long-term modeling or concerns about potential litigation. The ERO Enterprise data sampling recommended periods will not change if an entity retains documents, data, or information longer than the recommended periods, i.e. the scope of the data request will not go beyond recommended bounds, regardless of what data may be available at the entity.

The data retention team also addresses industry concerns that changes to the data retention requirements would be unduly burdensome, both in terms of financial and staffing considerations. Since the resulting requirement should be less extensive or simpler than that currently in place, any current policies would not need replacement. As stated above, data sampling requests will be limited to the data retention periods NERC sets, therefore entities will have time to either update their internal policies or leave them as is.

Based on the results of the comprehensive policy review, the data retention team recommends that NERC modify data retention requirements so that the burden of producing records necessary to demonstrate compliance is commensurate with the impact to the reliability of the BPS. Specifically, changes will be necessary in NERC Reliability Standard and RSAW development, as well as in audit or spot check data sampling.

Standard Development

Survey responses focused on clarity and consistency within the NERC Reliability Standards as primary areas of concern. The data retention team took this feedback into account and recommends all new Standards receive a default four-year data retention period. This four-year period will exclude the following:

- Voice and audio recordings, which will continue to be a 90-day rolling retention period.
- High-volume data, which would be restricted to a six-month rolling retention period.
- Standards requiring a current program or procedure, which would restrict to the currently effective version with a revision history specifying changes and dates of review.
- Standards requiring testing intervals (e.g. PRC-005), which would restrict to the most recent full testing records with evidence of previous testing intervals.

If current Reliability Standards are silent as to a data retention period, then the four-year or six-month data retention period should be used.

The data retention team is not recommending changing Standards slated for retirement. The Standards development teams will update existing Standards when they come up for review. This recommended change to the Standards will allow entities to set an automatic archival date for data, which should reduce storage space and data retention costs.

Auditor data sampling

Current guidance within the Auditor Manual states that registered entities must continue to demonstrate compliance for the entire audit period; however, the Auditor Manual does not define how the auditor should determine compliance with the NERC Reliability Standards.

---

14 See Appendix 6 Question 10.
Many industry concerns, as reflected in the survey responses, may be alleviated by incorporating the data retention white paper as a reference in the Auditor Manual, and issuing guidance to both the auditors and registered entities explaining how retention periods would apply in a Compliance Audit or Spot Check setting.

Guidance to auditors will need to make clear that while an entity may choose to retain some information for a longer period, the auditor requests should be limited to the data retention periods as established by NERC.

The data retention team recommends adding language to Section 03-0101 Preliminary Documentation review Action Item Tips & Techniques (figure 1), stating that, in general, auditors should focus their sampling of data to the most recent two years, unless the data sample would be statistically too small or irregularities are identified in the initial samples.

This limit would not apply to activity-based compliance that verifies periodic activities extending beyond the recommended two years or the audit period. This does not mean the auditor cannot sample and verify data throughout the whole audit period when, in the auditor’s professional judgment, it is necessary to confirm compliance.

### Action Item Tips & Techniques

1. Pre-evidence review methods...[text removed]
   a. Inquiry
   b. Observation
   c. Physical Examination
   d. Documentation Review
   e. Re-performance
   f. Confirmation
2. Available evidence may be limited by data retention requirements of the Reliability Standard or NERC guidance.
3. **Initial sampling of data should be focused on the most recent two years, unless the data sample would be statistically too small.**
4. Evidence of approval may be a physical signature, electronic signature/mark, or workflow process log.

**Figure 1: Recommended Manual language addition**

To promote consistency across the ERO Enterprise, NERC staff should continue to work with the Regional Entity audit staffs to develop a standard data-sampling methodology. This document should address evaluating the quality of implemented controls and statistically defensible data sample sizes and windows. This methodology should be shared with the industry so audited entities can better understand how to demonstrate compliance strategies. Moreover, implementing a consistent approach to sampling data may help address the perception and concerns expressed in the survey responses that “data requests appear to go beyond what was required in the standard and RSAW.”

Current RAI compliance activities are moving auditors to a risk-based (as opposed to compliance-based) view of monitoring. Auditors will continue to use professional judgment when requesting information older than two years. Auditors should recognize that with time comes reduced relevance, changing technologies, changing thresholds of evidence, changing regulatory interpretations, and an entity’s constant efforts to improve compliance performance. Finally, the Auditor Manual already includes sections detailing what should be included as a part of the working papers created during the audit.

Some of the information included in the working papers details data sampling and requests made during the audit, and Regional Entity audit processes. After instituting the changes to Standards and guidance to auditors, the ERO Enterprise should conduct a two-year review of these working papers, and compare them among Regional Entities in order to check for consistency and make any necessary further improvements.
Risk-based Enforcement

In order to implement fully a risk-based approach for compliance monitoring and enforcement, the current program is evolving more explicitly around the risk to reliability. Three goals of the RAI compliance monitoring program reinforce recommendations included in this white paper:

- Compliance monitoring should shift to using standard, risk-based audit practices similar to other industries.
- Audit scoping based on a standard approach to assessing an entity’s risk to reliability.
- Processes to allow lower-risk violations to stay in compliance space.

Beginning in November 2013, the ERO Enterprise implemented the first phase of the pilot program for Enforcement Discretion to identify minimal risk issues that registered entities would record and mitigate without triggering an enforcement action. The RAI program includes a project designed to develop guidelines for exercise of greater discretion in identifying when noncompliance requires formal enforcement action. The data retention team recommends focusing efforts on registered entities’ needs for a clearer understanding of what constitutes a higher risk\(^{15}\) that would require addressing noncompliance within the enforcement process.

To align data retention requirements to the risk-based goals of RAI, the data retention team recommends restricting duration of possible instances of noncompliance to the audit period. For example, if an entity has no evidence it ever complied with a NERC Reliability Standard, the duration period would default to the audit period. This recommendation aligns with the understanding that the relevance of noncompliance to reliability of the BPS decreases with time, and enforcing a duration of noncompliance past the most recent audit does not increase reliability or provide any additional protection to the BPS. Penalties for such violations should depend more on the risk of the violation than on its stated duration, in order to realize the deterrent value of monetary sanctions.

RSAW Improvements

To support consistency and reliability, the ERO Enterprise should establish an online resource with examples of acceptable evidence. The examples would not be the only ways to demonstrate compliance, but would provide tangible guidance to both the registered entities and auditors.

In addition, the ERO Enterprise should provide guidance to registered entities and auditors on alternative forms of compliance demonstration, such as attestations, to accommodate previously retained but deleted or archived data. Finally, there should be a method of providing feedback on RSAWs and auditing/spot-check processes to NERC and ensure there is a formal review of that feedback, as well as responsive recommendations from the ERO Enterprise.

Compliance communication tools redesign

Currently underway is the redesign of certain compliance communication tools. NERC and the Regional Entities are coordinating to provide formal and documented processes for creating and reviewing RSAWs. These improvements should produce more consistent audit processes for registered entities. In addition, the new processes will provide for an initial release of a draft RSAW in conjunction with the release of Reliability Standards for ballot and interaction between Standards and Compliance personnel during the drafting of Reliability Standards. In addition, NERC is developing a revised RSAW template to provide more complete information about audit procedures and evidence to registered entities.

\(^{15}\) Higher risk issues generally involve or result in: (a) extended outages, (b) loss of load, (c) cascading blackouts, (d) vegetation contacts, (e) systemic or significant performance failures, (f) intentional or willful acts or omissions, (g) gross negligence, or (h) other misconduct.
These new processes were announced within the ERO and to industry during the first quarter of 2014 and are expected to be fully implemented by the end of 2014.

**Required next steps**

There are no necessary changes to either the NERC Rules of Procedure or current and retired NERC Reliability Standards. The completed white paper will be presented to the CCC and provided as a reference to the RAI Auditor Manual Task Force and NERC Standards Department.
Chapter 4 – Conclusion

The data retention team identified and evaluated current data retention requirements and has used this white paper to recommend improvements to reduce the data-maintenance burdens on registered entities. The foundational principle of RAI is that it is not practical, effective, nor sustainable to monitor all compliance to the same degree. To this end, the future of registered entity data retention to demonstrate NERC compliance should not be retention for retention’s sake, but instead consistent with associated risk. Improvement will come in the form of incorporating consistent retention requirements into the standards development process and applying consistent ERO Enterprise-wide risk-based compliance monitoring practices.

While registered entities do need evidence to demonstrate compliance, the type of evidence and the retention period should match the updated RAI audit approach with the ultimate objective of assuring reliability. In implementing such measures, the ERO Enterprise and registered entities could reallocate resources to areas of greater risk to the reliability of the BPS. Feedback on the recommendations outlined in this white paper will focus and refine the ultimate data retention requirements and auditor sampling methodology. The approach to data retention improvements outlined herein utilizes flexibility in the audit approach and does not rely on changes to current NERC Reliability Standards or Rules of Procedure.