ERO ENTERPRISE

This is an interactive document.

Compliance Monitoring and Enforcement Manual

VERSION 4 | 2018

MANUAL | TABLE OF CONTENTS

VERSION 4 | 2018

COMPLIANCE MONITORING AND ENFORCEMENT MANUAL AND AUDITOR HANDBOOK | INFOGRAPHICS KEY

Manual >> Table of Contents

Auditor Handbook >> Key Documents to Complete

Auditor Handbook >> Table of Contents

Auditor Handbook >> Guiding Documents

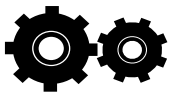
Manual >> Glossary

Auditor Handbook >> Task/Process Timing

Auditor Handbook >>
Audit Planning

Auditor Handbook >>
Audit Fieldwork

Auditor Handbook >>
Audit Reporting



Auditor Handbook >>
Action Item Steps

Auditor Handbook >>
Task/Action Item Highlights

Auditor Handbook >>
Action Item Tips and Techniques

Auditor Handbook >>
Action Item References

Auditor Handbook >>
Tasks

Auditor Handbook >>
Task/Action Item Highlights

FOREWORD

The ERO Compliance Monitoring and Enforcement Manual (Manual) documents the ERO Enterprise's current approaches used to assess a registered entity's compliance with the North American Electric Reliability Corporation (NERC) Reliability Standards and addresses sanctions and mitigations of confirmed violations. The creation of this Manual was possible through the efforts and collaboration of NERC and Regional Entity staff with the goal to improve the consistency and quality of CMEP activities across the ERO Enterprise. The Manual is a living document and will be revised as we continuously improve our processes.

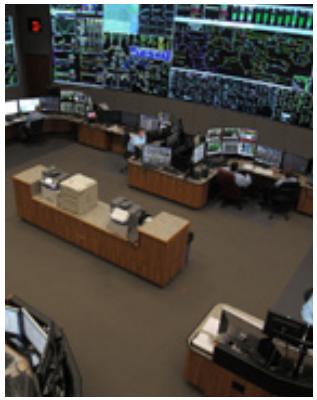
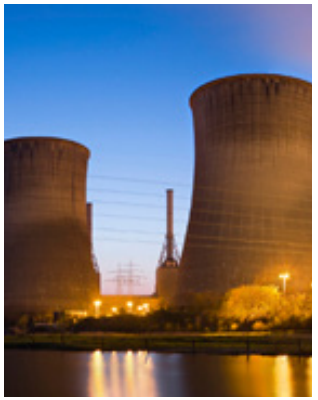
This Manual consists of several parts, and includes approaches and guidance related activities performed by ERO Enterprise staff under the Compliance Monitoring and Enforcement Program (CMEP). The Manual provides common tools, techniques, and methods for CMEP activities and the intended use of these tools is to drive consistency and to leverage best practices. At the same time, it must be recognized that due to the nature, diversity or complexity of the registered entities, this Manual does not address all the particular circumstances that may arise.

This Manual does not define how to determine compliance with the NERC Reliability Standards. This Manual also does not serve as a substitute for professional judgment, training, and experience.

Compliance Enforcement Authority staff are encouraged to forward comments or suggestions on the Manual to appropriate NERC and Regional Staff. Feedback can also be provided to ERO Enterprise Compliance Monitoring and Enforcement Manual Feedback.

ERO ENTERPRISE

Authoritative Guidance for CMEP Work

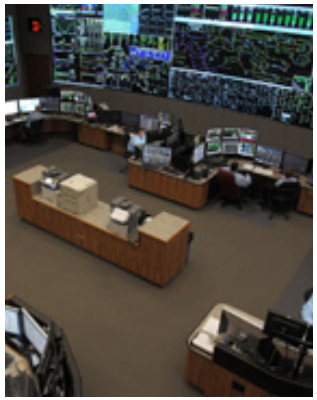
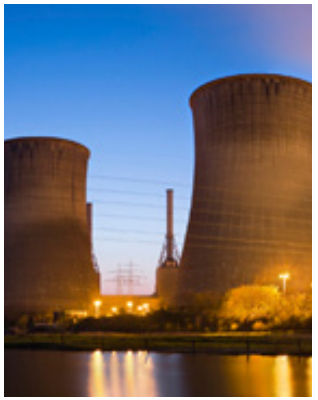



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

VERSION 4 | 2018

ERO ENTERPRISE

Authoritative Guidance for CMEP Work (Cont.)...

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

VERSION 4 | 2018

Chapter 2: General Standards for Performing CMEP Work (Cont.)...

- > Application of the Independence Conceptual Framework
- > Documentation of Independence
- > Professional Judgment
- > Competence
- > Technical Knowledge
- > Additional Qualifications for Critical Infrastructure Protection CMEP Work
- > Continuing Professional Education
- > Continuing Professional Education Requirements for Specialists
- > Quality Control and Assurance
- > System of Quality Control
- > Leadership Responsibilities for Quality within the CEA
- > Independence, Legal and Ethical Requirements
- > Initiation, Acceptance and Continuance of CMEP Work
- > Human Resources
- > CMEP Work Performance, Documentation and Reporting
- > Monitoring of Quality
- > Cross Reference: Authoritative Guidance vs. GAGAS

AUTHORITATIVE GUIDANCE FOR CMEP WORK | TABLE OF CONTENTS

PURPOSE AND BACKGROUND

The ERO Enterprise uses, "to the extent possible, the Generally Accepted Auditing Standards (GAAS), the Generally Accepted Government Auditing Standards (GAGAS), and standards sanctioned by the Institute of Internal Auditors, as guidance for performing activities under the Compliance Monitoring and Enforcement Program (CMEP)." While the ERO Enterprise does not necessarily perform audit activities that must be in accordance with these standards recognized in the United States, the ERO Enterprise uses these standards as framework to conduct compliance monitoring activities under the CMEP, and recognizes that these standards provide information used in oversight, accountability, transparency, and improvements in ERO Enterprise operations. As such, ERO Enterprise staff should be familiar with those standards applicable to the work performed under the CMEP.

The work associated with the CMEP provides essential accountability and transparency over compliance with regulatory-approved NERC Reliability Standards for the electric industry sector under federal and provincial law through the conduct of audits, enforcement and other activities. The design of the NERC Reliability Standards helps ensure the reliable operations of the Bulk Power System (BPS).

In the United States, Compliance Enforcement Authorities (CEAs), namely, NERC and the Regional Entities, under Section 215 of the Federal Power Act are required to monitor compliance with NERC Reliability Standards. Further, NERC and Regional Entities are required to assure its independence from those subject to the NERC Reliability Standards and provide fair and impartial procedures for enforcement of Reliability Standards.

For purposes of this Manual, the GAGAS principles and standards identified below apply to any CEA staff performing compliance monitoring and enforcement processes identified in the NERC Rules of Procedure, Appendix 4C. This section of the Manual highlights those specific chapters and areas within GAGAS that relates to CMEP work, specifically incorporating GAGAS Chapters 1 and 3. Other GAGAS chapters, as applicable, that do not appear in this section have been incorporated throughout this Manual and existing ERO Enterprise process guidance documents.

It is the policy of the ERO Enterprise that CEAs shall utilize and comply with appropriate GAGAS requirements, as identified in this section, in the performance of any activities governed by the CMEP, and that CEAs implement this policy within their organizations.

FOUNDATION AND ETHICAL PRINCIPLES FOR CMEP WORK | CHAPTER 1

Introduction

1-1 The concept of accountability for the use of delegated authority is key to governing processes. Management and staff entrusted with delegated authority are responsible for carrying out functions and providing service for the benefit of the public. Those functions should be done effectively, efficiently, economically, ethically, and equitably within the context of applicable law and the boundaries of the authority delegated.

1-2 The conduct of CMEP work is essential for providing reasonable assurance to government, industry, oversight bodies, and the public that compliance with Reliability Standards is being achieved, and that where violations or other areas of noncompliance occur, the matters are mitigated in a timely manner to reduce the risk to Reliable Operation of the BPS. It is equally essential to perform CMEP work in an independent, objective and transparent way.

Purpose and Applicability of Compliance Monitoring and Enforcement Standards and Guidance

1-3 The professional standards and guidance contained in GAGAS, and identified in this section, provide a framework for conducting CMEP work with competence, integrity, objectivity, and independence. These CMEP Standards and Guidance are applicable to CEA staff responsible for CMEP work.

1-4 CMEP work performed in accordance with this guidance provides information used for oversight, accountability, transparency, and improvement of Reliable Operations .[1] GAGAS is used to assist CEA staff in objectively acquiring and evaluating sufficient, appropriate evidence, reporting the results, and making determinations about compliance exceptions and enforcement.

1-5 This document establishes CEA policy for assuring integrity in the conduct and oversight of CMEP work. It is the policy of the Compliance Enforcement Authorities that CEA staff shall utilize and comply with appropriate Yellow Book requirements, as described within this document, in the performance of CMEP-related work and that CEA management shall implement this policy within their organizations. Further, NERC shall monitor and assure compliance with this policy by Regional Entities.

[1] Reliable Operations, as defined in the NERC Glossary of Terms, located: http://www.nerc.com/files/glossary_of_terms.pdf

FOUNDATION AND ETHICAL PRINCIPLES FOR CMEP WORK | CHAPTER 1

Ethical Principles

1-6 The ethical principles presented in this section provide the foundation, discipline, and structure, as well as the climate that influences the application of GAGAS. This section sets forth fundamental principles rather than establishing specific standards or requirements.

1-7 Because the CEA operates under authority from government, the public expects the CEA to conduct work in accordance with GAGAS and to follow its ethical principles. Management of the CEA sets the tone for ethical behavior throughout the organization by maintaining an ethical culture, clearly communicating acceptable behavior and expectations to each employee, and creating an environment that reinforces and encourages ethical behavior throughout all levels of the organization. The ethical tone maintained and demonstrated by management and staff is an essential element of a positive ethical environment for the CEA.

1-8 Conducting CMEP work in accordance with ethical principles is a matter of personal and organizational responsibility. Ethical principles apply in preserving CEA staff independence, taking on only that work which the CEA is competent to perform, performing high-quality work, and following the applicable standards. Integrity and objectivity are maintained when CEA staff perform the work and make decisions that are consistent with the broader interest of those relying on the CEA's work, including the public.

1-9 Other ethical requirements or codes of professional conduct may also be applicable to CEA staff that perform CMEP work in accordance with GAGAS. For example, individual CEA staff may be members of professional organizations or licensed or certified professionals who are also subject to ethical requirements of those professional organizations or licensing bodies.

1-10 The ethical principles that guide the work of CEA staff who conduct CMEP work in accordance with GAGAS are:

a. the public interest;
b. integrity;
c. objectivity;
d. proper use of information, resources, and positions; and
e. professional behavior.

FOUNDATION AND ETHICAL PRINCIPLES FOR CMEP WORK | CHAPTER 1

The Public Interest

1-11 The public interest is defined as the collective well-being of the community of people and entities served by the CEA. The public interest is best served by achieving the mission of the CEAs, namely, assurance of Reliable Operation of the BPS. Observing integrity, objectivity, and independence in discharging professional responsibilities assists CEA staff in meeting the principle of serving the public interest and honoring the public trust. The principle of the public interest is fundamental to the responsibilities of CEA staff and critical in the delegated authority environment.

1-12 A distinguishing mark of a CEA staff member is acceptance of responsibility to serve the public interest. This responsibility is critical when performing CMEP work in the CEA environment. GAGAS embodies the concept of accountability, which is fundamental to serving the public interest.

Integrity

1-13 Public confidence in the CEA is maintained and strengthened by CEA staff performing professional responsibilities with integrity. Integrity includes CEA staff conducting the work with an attitude that is objective, fact-based, nonpartisan, and non-ideological with regard to registered entities and users of the CEA staff's reports. Within the constraints of applicable confidentiality laws, rules, or policies, communications with the registered entity, those charged with governance, and the individuals contracting for or requesting work under the CMEP are expected to be honest, candid, and constructive.

1-14 Making decisions consistent with the public interest of the program or activity subject to CMEP work is an important part of the principle of integrity. In discharging their professional responsibilities, CEA staffs may encounter concurrent, conflicting interpretations of evidence, pressure from management of both registered entity and CEA management, various levels of government, and other impacted entities, and, potentially, pressure to inappropriately achieve personal or organizational gain. In resolving those conflicts and pressures, acting with integrity means that CEA staff exhibit impartiality and maturity and place priority on their responsibilities to the public interest.

Objectivity

1-15 The credibility of the CMEP work is based on CEA staff's objectivity in discharging their professional responsibilities. Objectivity includes independence of mind and appearance when providing services under GAGAS, maintaining an attitude of impartiality, having intellectual honesty, and being free of conflicts of interest. Maintaining objectivity includes a continuing assessment of relationships with registered entities and other stakeholders in the context of the CEA staff's responsibility to the public. The concepts of objectivity and independence are closely related. Independence impairments impact objectivity.

Proper Use of Information, Resources and Positions

1-16 CMEP information, resources, and positions are to be used for CEA purposes only and not inappropriately for CEA staff members' personal gain or in a manner contrary to law or detrimental to the legitimate interests of the Registered Entity or the CEA. This concept includes the proper handling of sensitive or classified information or resources.

1-17 In the delegated authority environment, the public's right to the transparency of information has to be balanced with the proper use of that information. In addition, much of the CMEP work is subject to laws and regulations dealing with the disclosure of information. To accomplish this balance, exercising discretion in the use of information acquired in the course of CEA staff's duties is an important part in achieving this goal. Improperly disclosing any such information to third parties is not an acceptable practice.

1-18 Accountability to the public for the proper use and prudent management of government resources is an essential part of CEA staff's responsibilities. Protecting and conserving CEA resources and using them appropriately for authorized activities are important elements in the public and industry's expectations for CEA staff.

1-19 Misusing the position of a CEA staff member for financial gain or other benefit violates a CEA staff member's fundamental responsibilities. Credibility can be damaged by actions that could be perceived by an objective third party with knowledge of the relevant information as improperly benefiting a CEA staff member's personal financial interests or those of an immediate or close family member; a general partner; an organization for which the CEA staff member serves as an officer, director, trustee, or employee; or an organization with which the CEA staff member is negotiating concerning future employment.

Professional Behavior

1-20 High expectations for professionals doing CMEP work include compliance with all relevant legal, regulatory, and professional obligations and avoidance of any conduct that might bring discredit to CEA staff's work, including actions that would possibly create an appearance of impropriety. Above all, professional behavior involves CEA staff putting forth an honest and competent effort in performance of their duties and professional services.

GENERAL STANDARDS FOR PERFORMING CMEP WORK | CHAPTER 2

Introduction

2-1 This chapter establishes general standards and provides guidance for performing work under the CMEP. These general standards, along with the overarching ethical principles presented in chapter One, establish a foundation for the credibility of CEA staff's work. These general standards emphasize the importance of the independence of the CEA and its individual CEA staff members; the exercise of professional judgment in the performance of work and the preparation of related reports; the competence of staff; and quality control and assurance. In all matters relating to the CMEP work, the CEA and the individual CEA staff member, regardless of governance structure, must be independent.

Independence

2-2 Independence is comprised of two components:

a. **Independence of Mind.** The state of mind that permits the performance of CMEP work without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism.

b. **Independence in Appearance.** The absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of a CEA staff member had been compromised.

2-3 CEA staff and the CEA maintain independence so that their opinions, findings, conclusions, judgments, and recommendations will be impartial and viewed as impartial by reasonable and informed third parties. CEA staff should avoid situations that could lead reasonable and informed third parties to conclude that the CEA staff members are not independent and thus are not capable of exercising objective and impartial judgment on all issues associated with conducting the CMEP work and reporting on the work.

2-4 CEA staff should be independent from a registered entity during:

a. any period of time that falls within the period covered by the CMEP work or subject matter of the work, and
b. the period of the start of the CMEP work, which begins when the CEA staff members are assigned to the work. The period lasts for the entire duration that the registered entity is subject to the jurisdiction of the CEA.

Compliance Monitoring and Enforcement Program Standards and Guidance Conceptual Framework Approach to Independence

2-5 Many different circumstances, or combinations of circumstances, are relevant in evaluating threats to independence. Therefore, GAGAS establishes a conceptual framework that CEA staff can use to identify, evaluate, and apply safeguards to address threats to independence. The conceptual framework assists CEA staff in maintaining both independence of mind and independence in appearance. It can be applied to many variations in circumstances that create threats to independence and allows CEA staff to address threats to independence that result from activities that are not specifically prohibited by GAGAS.

2-6 CEA staff should apply the conceptual framework for all CMEP work at the CEA and individual CEA staff levels to:

a. identify threats to independence;
b. evaluate the significance of the threats identified, both individually and in the aggregate; and
c. apply safeguards as necessary to eliminate the threats or reduce them to an acceptable level.

2-7 If no safeguards are available to eliminate an unacceptable threat or reduce it to an acceptable level, independence would be considered impaired.

2-8 For consideration of CEA staff independence, offices or units of the CEA, or related or affiliated entities under common control, are not differentiated from one another. Consequently, for the purposes of independence evaluation using the conceptual framework, to the extent that the CEA includes multiple offices or units, or includes multiple entities related or affiliated through common control, it is considered to be one CEA.

Threats to Independence[2]

2-9 The following sections discuss threats to independence, safeguards or controls to eliminate or reduce threats, and application of the conceptual framework for independence.

2-10 Threats to independence are circumstances that could impair independence. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise a CEA staff member's professional judgment or create the appearance that the CEA staff member's professional judgment may be compromised, and on the specific safeguards applied to eliminate the threat or reduce it to an acceptable level. Threats are conditions to be evaluated using the conceptual framework. Threats do not necessarily impair independence.

2-11 Threats to independence may be created by a wide range of relationships and circumstances. CEA staff should evaluate the following broad categories of threats to independence when threats are being identified and evaluated.

a. Self-interest threat: the threat that a financial or other interest will inappropriately influence a CEA staff member's judgment or behavior.
b. Self-review threat: the threat that CEA staff that has provided previous work within the CEA or external to the CEA will not appropriately evaluate the results of previous judgments made or services performed as part of the previous work when forming a judgment significant to a CMEP determination.
c. Bias threat: the threat that a CEA staff member will, as a result of political, ideological, social, or other convictions, take a position that is not objective.
d. Familiarity threat: the threat that aspects of a relationship with management or personnel of a Registered Entity, such as a close or long relationship, or that of an immediate or close family member, will lead a CEA staff member to take a position that is not objective.
e. Undue influence threat: the threat that external influences or pressures will impact a CEA staff member's ability to make independent and objective judgments.
f. Management participation threat: the threat that results from CEA staff taking on the role of management or otherwise performing management functions on behalf of the entity undergoing a CMEP action.
g. Circumstances that result in a threat to independence in one of the above categories may result in other threats as well. For example, a circumstance resulting in a familiarity threat to independence may also expose other CEA staff members to undue influence threats.

[2] CEAs are expected to maintain policies and procedures that assure integrity and independence of their respective programs and as part of its CMEP work per the Amended and Restated Delegation Agreements between NERC and the Regional Entities and Appendix 4C of the NERC RoP.

Safeguards

2-12 Safeguards are controls designed to eliminate, or reduce to an acceptable level, threats to independence. Under the conceptual framework, the CEA staff applies safeguards that address the specific facts and circumstances under which threats to independence exist. In some cases, multiple safeguards may be necessary to address a threat. The list of safeguards in this section provides examples that may be effective under certain circumstances. The list cannot provide safeguards for all circumstances. It does, however, provide a starting point for considering what safeguards could eliminate those threats that have been identified or reduce them to an acceptable level.

2-13 Examples of CMEP safeguards include:

a. consulting an independent third party, such as a professional organization, a professional regulatory body, or another CEA staff;
b. involving another CEA staff or independent third party to perform or re-perform part of the work;
c. having a professional staff member who was not a member of the team review the work performed; and
d. removing an individual from a team when that individual's financial or other interests or relationships pose a threat to independence.

Depending on the nature of the monitoring activity, CEA staff may also be able to place limited reliance on safeguards that the entity has implemented.

2-14 Examples of safeguards within the CEA's systems and procedures include:

a. internal procedures that ensure objective choices in making determinations, including staff assignments, under the CMEP; and
b. a governance structure that provides appropriate oversight and communications regarding the performance of CMEP work and use of the Yellow Book requirements.

Application of the Independence Conceptual Framework

2-15 CEA staff should evaluate threats to independence using the conceptual framework when the facts and circumstances under which the CEA staff performs the work may create or augment threats to independence. CEA staff should evaluate threats both individually and in the aggregate because threats can have a cumulative effect on a CEA staff's independence.

2-16 Facts and circumstances that create threats to independence can result from events such as the start of a new engagement or the assignment of new staff member to a CMEP work project. Many other events can result in threats to independence. CEA staff uses professional judgment to determine whether the facts and circumstances created by an event warrant use of the conceptual framework. Whenever relevant new information about a threat to independence comes to the attention of the CEA staff during the course of CMEP work, the CEA staff should evaluate the significance of the threat in accordance with the conceptual framework.

2-17 CEA staff should determine whether identified threats to independence are at an acceptable level or have been eliminated or reduced to an acceptable level. A threat to independence is not acceptable if it either (a) could impact the CEA staff member's ability to perform the work without being affected by influences that compromise professional judgment, or (b) could expose the CEA staff or the CEA to circumstances that would cause a reasonable and informed third party to conclude that the integrity, objectivity, or professional skepticism of the CEA, or a CEA staff member, had been compromised.

2-18 When a CEA staff identifies threats to independence, and based on an evaluation of those threats determines that they are not at an acceptable level, the CEA staff should determine whether appropriate safeguards are available and can be applied to eliminate the threats or reduce them to an acceptable level. The CEA staff should exercise professional judgment in making that determination, and should take into account whether both independence of mind and independence in appearance are maintained. The CEA staff should evaluate both qualitative and quantitative factors when determining the significance of a threat.

2-19 In cases where threats to independence are not at an acceptable level, thereby requiring the application of safeguards, the CEA staff should document the threats identified and the safeguards applied to eliminate the threats or reduce them to an acceptable level.

2-20 Certain conditions may lead to threats that are so significant that they cannot be eliminated or reduced to an acceptable level through the application of safeguards, resulting in impaired independence. Under such conditions, CEA staff should seek alternatives or terminate the CMEP work.

Application of the Independence Conceptual Framework (Cont.)...

2-21 If a threat to independence is initially identified after the CEA staff's CMEP compliance monitoring work is complete, then CEA staff should evaluate the threat's impact on the CMEP work and on compliance with GAGAS. If the CEA staff determines that the newly identified threat had an impact on the CMEP work that would have resulted in the outcome of the CEA staff's CMEP compliance monitoring work being different had the CEA staff been aware of it, they should communicate in the same manner as that used to originally distribute the results of the CMEP compliance monitoring work to those charged with CMEP governance and the appropriate officials of the registered entity, and other known users, so that they do not continue to rely on findings or conclusions that were impacted by the threat to independence.

If the results of the CMEP compliance monitoring work or determination was previously posted to the CEA's publicly accessible website, the CEA staff should remove the results of the CMEP compliance monitoring work and post a public notification that the results of the CMEP compliance monitoring work was removed. The CEA staff should then determine whether to conduct additional CMEP work necessary to reissue the results of the CMEP compliance monitoring work, including any revised findings, determinations or conclusions or repost the original results of the CMEP compliance monitoring work and/or determination if the additional CMEP work does not result in a change in findings or conclusions.

2-22 Whether an activity is a registered entity management responsibility depends on the facts and circumstances and CEA staff's exercise of professional judgment in identifying these activities. Examples of activities that are considered management responsibilities and would therefore impair independence if performed for a registered entity include:

a. setting policies and strategic direction for the registered entity;
b. directing and accepting responsibility for the actions of the registered entity's employees in the performance of their routine, recurring activities;
c. having custody of a registered entity's assets;
d. reporting to those charged with governance on behalf of management;
e. deciding which of the CEA staff's or outside third party's recommendations to implement;
f. accepting responsibility for the management of a registered entity's project;
g. accepting responsibility for designing, implementing, or maintaining internal control;
h. providing services that are intended to be used as management's primary basis for making decisions that are significant to the subject matter of Reliability Standards or other CMEP work;
i. developing a registered entity's performance measurement system when that system is material or significant to
j. Reliability Standards and/or the subject matter of the CMEP work; and
k. serving as a voting or ex officio member of a registered entity's management committee or board of directors.

Documentation of Independence

2-23 Documentation of independence considerations provides evidence of the CEA staff's judgments in forming conclusions regarding compliance with independence requirements. GAGAS contains specific requirements for documentation related to independence which may be in addition to the documentation that CEA staff has previously maintained. While insufficient documentation of CEA staff's compliance with the independence standard does not impair independence, appropriate documentation is required under the GAGAS quality control and assurance requirements.

The independence standard includes the following documentation requirements:

a. document threats to independence that require the application of safeguards, along with safeguards applied, in accordance with the conceptual framework for independence; and
b. document consideration of registered entity management's ability to effectively oversee the CMEP work to be provided to the CEA staff.

Professional Judgment

2-24 CEA staff must use professional judgment in planning and performing CMEP work and in reporting the results.

2-25 Professional judgment includes exercising reasonable care and professional skepticism. Reasonable care includes acting diligently in accordance with applicable professional standards and ethical principles. Professional skepticism is an attitude that includes a questioning mind and a critical assessment of evidence. Professional skepticism includes a mindset in which CEA staff assumes management is neither dishonest nor of unquestioned honesty.

2-26 Using the CEA staff's professional knowledge, skills, and experience to diligently perform, in good faith and with integrity, the gathering of information and the objective evaluation of the sufficiency and appropriateness of evidence is a critical component of CMEP work. Professional judgment and competence are interrelated because judgments made are dependent upon the CEA staff's competence.

Professional Judgment (Cont.)...

2-27 Professional judgment represents the application of the collective knowledge, skills, and experiences of all the personnel involved with a CMEP work project, as well as the professional judgment of individual CEA staff members. In addition to personnel directly involved, professional judgment may involve collaboration with other stakeholders, external specialists, and management in the CEA.

Using professional judgment is important to the ability of CEA staff to carry out all aspects of professional responsibilities, including following the independence standards and related conceptual framework; maintaining objectivity and credibility; assigning competent staff to the CMEP work; defining the scope of work; evaluating, documenting, and reporting the results of the work; and maintaining appropriate quality control over CMEP work performed.

2-28 Using professional judgment is important to CEA staff in applying the conceptual framework to determine independence in a given situation. This includes the consideration of any threats to the CEA staff member's independence and related safeguards which may mitigate the identified threats. CEA staff use professional judgment in identifying and evaluating any threats to independence, including threats to the appearance of independence. [3]

2-29 Using professional judgment is important to CEA staff in determining the required level of understanding of the subject matter and related circumstances. This includes consideration about whether the CEA staff's collective experience, training, knowledge, skills, abilities, and overall understanding are sufficient to assess the risk that the subject matter of the CMEP work may contain a significant inaccuracy or could be misinterpreted.

2-30 CEA staff's consideration of the risk level of each CMEP work project, including the risk of arriving at improper conclusions, is also important. Within the context of CMEP risk, exercising professional judgment in determining the sufficiency and appropriateness of evidence to be used to support the findings and conclusions based on the Reliability Standards and any recommendations reported is an integral part of the process.

2-31 While this standard places responsibility on each CEA staff member and the CEA to exercise professional judgment in planning and performing CMEP work, it does not imply unlimited responsibility, nor does it imply infallibility on the part of either the individual CEA staff member or the CEA. Absolute assurance is not attainable due to factors such as the nature of evidence and characteristics of fraud. Professional judgment does not mean eliminating all possible limitations or weaknesses associated with a specific CMEP work project, but rather identifying, assessing, mitigating, and explaining them.

[3] See paragraph **2.4** for a description of independence in appearance.

GENERAL STANDARDS FOR PERFORMING CMEP WORK | CHAPTER 2

Competence

2-32 The staff assigned to perform the CMEP work must collectively possess adequate professional competence needed to address the Reliability Standards and perform the work in accordance with GAGAS.

2-33 The CEA's management should assess skill needs to consider whether its workforce has the essential skills that match those necessary to perform the particular CMEP work. Accordingly, the CEA should have a process for recruitment, hiring, continuous development, assignment, and evaluation of staff to maintain a competent workforce.

2-34 Competence is derived from a blending of education and experience. Competencies are not necessarily measured by years of relevant experience because such a quantitative measurement may not accurately reflect the kinds of experiences gained by a CEA staff in any given time period. Maintaining competence through a commitment to learning and development throughout a CEA staff member's professional life is an important element for CEA staff. Competence enables CEA staff to make sound professional judgments.

Technical Knowledge

2-35 The staff assigned to conduct CMEP work in accordance with GAGAS should collectively possess the technical knowledge, skills, and experience necessary to be competent for the type of work being performed before beginning work on that project. The staff assigned to conduct CMEP work under GAGAS should collectively possess:

a. knowledge of GAGAS applicable to the type of work they are assigned and the education, skills, and experience to apply this knowledge to the work being performed;
b. general knowledge of the environment in which the Registered Entity operates and the subject matter;
c. skills to communicate clearly and effectively, both orally and in writing; and
d. skills appropriate for the work being performed; for example, skills in:

1) statistical or non-statistical sampling if the work involves use of sampling;
2) information technology, including controls systems, if the work involves review of information systems and/or controls systems;
3) engineering if the work involves review of complex engineering data;
4) specialized audit methodologies or analytical techniques, such as the use of complex survey instruments, model-based estimates, or statistical analysis tests, as applicable; or
5) specialized knowledge in subject matters, such as power systems state estimation, real-time contingency analysis, system planning, or any other specialized subject matter, if the work calls for such expertise.

Additional Qualifications for Critical Infrastructure Protection CMEP Work

2-36 CEA staff performing Critical Infrastructure Protection CMEP work under the GAGAS should be knowledgeable in network systems, communications, and firewalls, for example, and carry appropriate certifications.

Continuing Professional Education

2-37 CEA staff performing work in accordance with GAGAS, including planning, directing, performing CMEP work procedures, or reporting on CMEP work conducted in accordance with GAGAS, should maintain professional competence through continuing professional education. Therefore, each CEA staff member performing CMEP work should follow the guidance and meet the requirements specifically outlined by the ERO Enterprise.

2-38 Meeting continued professional education requirements is primarily the responsibility of individual CEA staff member. The CEA should have quality control procedures to help ensure that CEA staff members meet the continuing education requirements, including documentation of the continuing education completed.

Continuing Professional Education Requirements for Specialists

2-39 The CEA should determine that external specialists assisting in performing CMEP work under the GAGAS are qualified and competent in the specialist's areas of specialization.

Quality Control and Assurance

2-40 Each CEA performing CMEP work in accordance with GAGAS must establish and maintain a system of quality control that is designed to provide the CEA with reasonable assurance that the organization and its personnel comply with professional standards and applicable legal and regulatory requirements.

System of Quality Control

2-41 A CEA's system of quality control encompasses the CEA's leadership, emphasis on performing high quality work, and the policies and procedures designed to provide reasonable assurance of complying with professional standards and applicable legal and regulatory requirements. The nature, extent, and formality of the CEA's quality control systems will vary based on the CEA's circumstances, such as geographic dispersion, knowledge and experience of its personnel, nature and complexity of its CMEP work, and cost-benefit considerations.

2-42 Each CEA should document its quality control policies and procedures and communicate those policies and procedures to its personnel. The CEA should document compliance with its quality control policies and procedures and maintain such documentation for a period of time sufficient to enable those performing monitoring procedures to evaluate the extent of the CEA's compliance with its quality control policies and procedures. The form and content of such documentation are a matter of professional judgment and will vary based on the CEA's circumstances.

2-43 The CEA should establish policies and procedures in its system of quality control that collectively address:

a. leadership responsibilities for quality within the CEA;
b. independence, legal, and ethical requirements;
c. initiation, acceptance, and continuance of CMEP work;
d. human resources;
e. CMEP work performance, documentation, and reporting; and
f. monitoring of quality.

Leadership Responsibilities for Quality within the CEA

2-44 The CEA should establish policies and procedures on leadership responsibilities for quality within the CEA that include the designation of responsibility for quality of the CMEP work performed in accordance with GAGAS and communication of policies and procedures relating to quality. Appropriate policies and communications encourage a culture that recognizes that quality is essential in performing CMEP work under GAGAS and that leadership of the CEA is ultimately responsible for the system of quality control.

2-45 The CEA should establish policies and procedures designed to provide it with reasonable assurance that those assigned operational responsibility for the CEA's system of quality control have sufficient and appropriate experience and ability, and the necessary authority, to assume that responsibility.

GENERAL STANDARDS FOR PERFORMING CMEP WORK | CHAPTER 2

Independence, Legal and Ethical Requirements

2-46 The CEA should establish policies and procedures on independence, legal, and ethical requirements that are designed to provide reasonable assurance that the CEA and its personnel maintain independence and comply with applicable legal and ethical requirements. Such policies and procedures assist the CEA to:

a. communicate its independence requirements to its staff; and
b. identify and evaluate circumstances and relationships that create threats to independence, and take appropriate action to eliminate those threats or reduce them to an acceptable level by applying safeguards, or, if considered appropriate, withdraw from the CMEP work project where withdrawal is not prohibited by law or regulation.

Initiation, Acceptance and Continuance of CMEP Work

2-47 The CEA should establish policies and procedures for the initiation, acceptance, and continuance of CMEP work that are designed to provide reasonable assurance that the CEA will undertake the work only if it can comply with professional standards, legal requirements, and ethical principles and is acting within the legal mandate or authority of the CEA.

GENERAL STANDARDS FOR PERFORMING CMEP WORK | CHAPTER 2

Human Resources

2-48 The CEA should establish policies and procedures for human resources that are designed to provide the CEA with reasonable assurance that it has personnel with the capabilities and competence to perform the CMEP work in accordance with professional standards and legal and regulatory requirements.

CMEP Work Performance, Documentation and Reporting

2-49 The CEA should establish policies and procedures for CMEP work performance, documentation, and reporting that are designed to provide the CEA with reasonable assurance that the CMEP work is performed and reports are issued in accordance with professional standards and legal and regulatory requirements.

2-50 When performing CMEP work under GAGAS, the CEA should have policies and procedures for the safe custody and retention of CMEP work documentation for a time sufficient to satisfy legal, regulatory, and administrative requirements for records retention. Whether CMEP work documentation is in paper, electronic, or other media, the ability to retrieve, as well as the integrity and accessibility of the underlying information could be compromised if the documentation is altered, added to, or deleted without CEA staff's knowledge, or if the documentation is lost or damaged. For CMEP work documentation that is retained electronically, the CEA should establish effective information systems controls concerning accessing and updating the CMEP work documentation.

Monitoring of Quality

2-51 The CEA should establish policies and procedures for monitoring of quality. Monitoring of quality is an ongoing, periodic assessment of work completed on CMEP work designed to provide management of the CEA with reasonable assurance that the policies and procedures related to the system of quality control are suitably designed and operating effectively in practice. The purpose of monitoring compliance with quality control policies and procedures is to provide an evaluation of whether the:

a. professional standards and legal and regulatory requirements have been followed;
b. quality control system has been appropriately designed; and
c. quality control policies and procedures are operating effectively and complied with in practice.

2-52 Monitoring procedures will vary based on the CEA's facts and circumstances. The CEA should perform monitoring procedures that enable it to assess compliance with applicable professional standards and quality control policies and procedures for CMEP work performed under GAGAS. Individuals performing monitoring should collectively have sufficient expertise and authority for this role.

2-53 The CEA should analyze and summarize the results of its monitoring process at least annually, with identification of any systemic or repetitive issues needing improvement, along with recommendations for corrective action. The CEA should communicate to appropriate personnel any deficiencies noted during the monitoring process and make recommendations for appropriate remedial action.

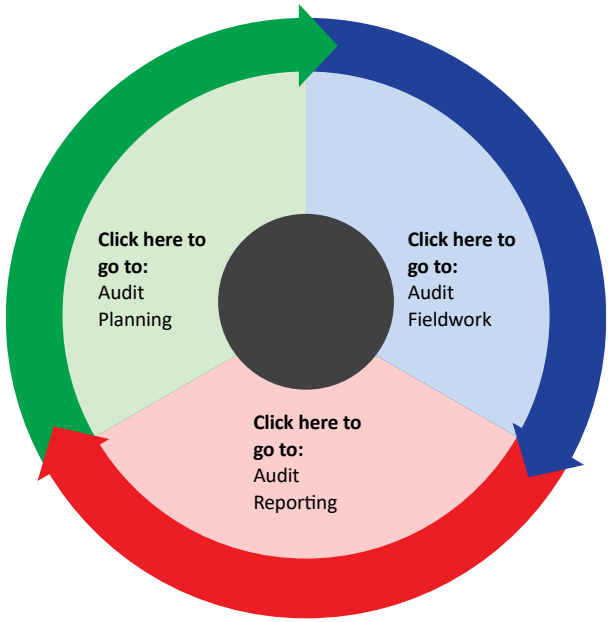
Authoritative Guidance vs. GAGAS

Authoritative Guidance Section	GAGAS Section(s)
1.1	N/A
1.2	N/A
1.3	1.04
1.4	1.05
1.5	N/A
1.6	1.10
1.7	1.11
1.8	1.12
1.9	1.13
1.10	1.14
1.11	1.15
1.12	1.16
1.13	1.17
1.14	1.18
1.15	1.19
1.16	1.20
1.17	1.21
1.18	1.22
1.19	1.23
1.20	1.24
2.1	3.01
2.2	3.03
2.3	3.04
2.4	3.05
2.5	3.07
2.6	3.08
2.7	3.09
2.8	3.10
2.9	3.12
2.10	3.13
2.11	3.14
2.12	3.16
2.13	3.17 & 3.18
2.14	3.19
2.15	3.20
2.16	3.21
2.17	3.22

Authoritative Guidance Section	GAGAS Section(s)
2.18	3.23
2.19	3.24
2.20	3.25
2.21	3.26
2.22	3.36
2.23	3.59
2.24	3.60
2.25	3.61
2.26	3.62
2.27	3.63 & 3.64
2.28	3.65
2.29	3.66
2.30	3.67
2.31	3.68
2.32	3.69
2.33	3.70
2.34	3.71
2.35	3.72
2.36	N/A
2.37	3.76
2.38	3.78
2.39	3.79
2.40	3.82
2.41	3.83
2.42	3.84
2.43	3.85
2.44	3.86
2.45	3.87
2.46	3.88
2.47	3.89
2.48	3.90
2.49	3.91
2.50	3.92
2.51	3.93
2.52	3.94
2.53	3.95

ERO ENTERPRISE

Auditor Handbook and Checklist



VERSION 4 | 2018

To ensure the reliability of the BPS, users, owners and operators are subject to compliance of NERC Reliability Standards. Each organization must be able to demonstrate compliance through the existence of sufficient and appropriate evidence. The Handbook represents the collaborative efforts of the ERO-Enterprise to develop a companion document for the Auditor Checklist. Opportunities have been identified to strengthen the Auditor Checklist through aligning process steps and clarifying language.

A compliance audit is a comprehensive review of an organization's adherence to NERC Reliability Standards and/or Regional Reliability Standards which have been developed by the users, owners and operators of the BPS and been approved by FERC and other regulatory agencies in the form of a standard. A compliance audit provides reasonable assurance the registered entity is following the rules and meeting requirements of a standard. It will also help identify weak or problem areas, so the registered entities can take necessary steps to restore the organization to conformity with the standards.

NERC Compliance auditing determines whether a registered entity has met applicable requirements. For each standard/requirement examined, the compliance auditor decides whether or not it complies with the chosen standard/requirement. The auditor reports reasons for noncompliance, if found; and describes implications and risks of noncompliance.

Before beginning a particular compliance audit, the auditors must be properly qualified through education and experience to perform the work. The auditor must have an understanding of the nature, purpose, objectives, and scope of the compliance audit. The auditor should obtain a thorough understanding of the standards being evaluated, be able to recognize when a deviation has occurred, and know how to evaluate evidence obtained through testing. Detailed information about key compliance audit questions often exists in the form of independently published compliance audit guidelines and generally accepted auditing standards. The ERO-Enterprise uses the Generally Accepted Government Accounting Standards (GAGAS), the Institute of Internal Auditing (IIA) and the International Professional Practices Framework (IPPF) as guides for audit engagements.

The scope of a NERC compliance audit will be determined by the registered entity's Inherent Risk Assessment, the optional Internal Control Evaluation, and identified Regional risks.

The purpose of the Handbook is to be a companion document that supports the activities identified in the Auditor Checklist.

The goals of the Handbook are to:

- Create consistent regional audit practices needed to complete comprehensive and rigorous compliance audits
- Derive content from authoritative guidance promulgated by recognized organizations
- Serve new and tenured auditors alike
- Determine responsibility, authority, and accountability for each action item on the Auditor Checklist
- Support auditor judgment to drive consistency of approach in a defensible manner
- Function on a laptop or tablet as a sound reference document
- Be an expandable and upgradeable document

The Handbook is not intended to be a fully comprehensive document, nor does it limit auditor judgment. It does not define how to determine compliance with NERC Reliability Standards. However, it does define procedural steps required to perform an audit and promotes consistency between the regions.

The Handbook follows the organization of the Auditor Checklist and consists of three primary Areas, Tasks that support the Areas, and Action Items to support the Tasks. The Areas, Tasks, and Action Items comprise the Audit Cycle.

The primary Areas are: Audit Planning, Audit Fieldwork, and Audit Reporting which make up the Audit Cycle. The Glossary is included to define terms used in the Handbook.

The Handbook contains Areas, Tasks, and Action Items for completion. Each Task reviews the required action and highlights for the Compliance Auditor to reference. Each Action Item details specific steps that allow the Compliance Auditor, Audit Team Lead, Compliance Support, and Management to complete the Auditor Checklist item. Action Items also provide tips and techniques to consider, as well as specific professional guidance that supports the necessity of the action.

The following is a brief explanation of each Area in the Handbook which addresses the Audit Cycle at a high level.

- **Audit Planning** – assures the audit team addresses the development of the objective related to risk, scope, and other necessary documentation and approaches for the implementation of the fieldwork.

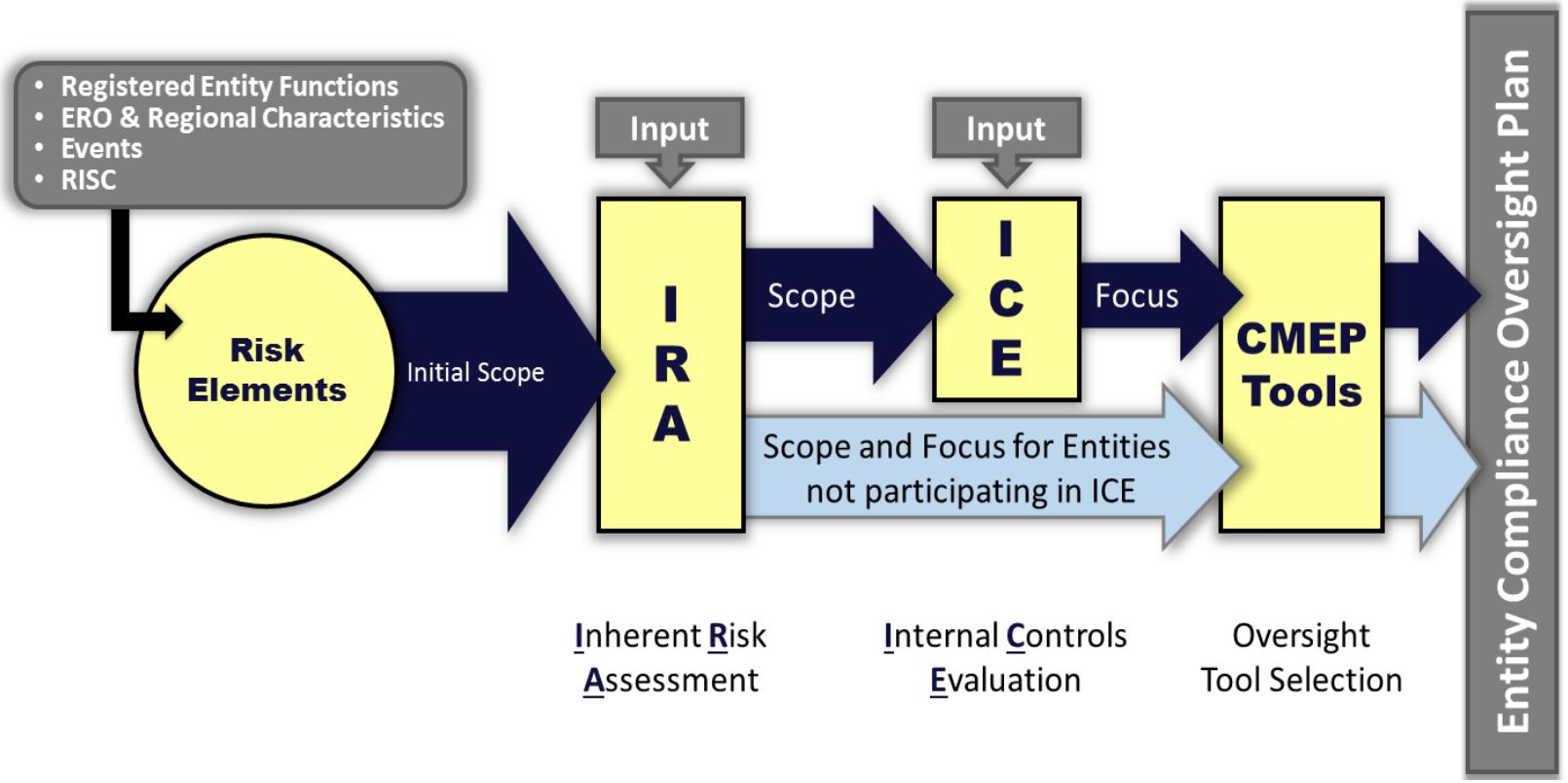
- **Audit Fieldwork** – assures the audit team performs Action Items to conduct the audit, communicate with the entity, and document results.

- **Audit Reporting** – assures the audit team performs Action Items to develop and publish the report.

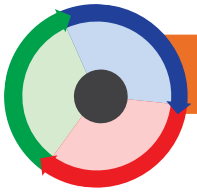
The Auditor Handbook and Checklist are living documents and will be monitored and maintained by a team of auditors. Changes to the handbook and checklist may be made as comments are received from regional implementation and risk-based monitoring.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Risk Based Process Flow



1 Reference Functional Model at http://www.nerc.com/pa/Stand/Pages/FunctionalModel.aspx **and** Registration Information at http://www.nerc.com/pa/comp/Pages/Registration.aspx
2 Reference current year ERO CMEP Implementation Plan at: http://www.nerc.com/pa/comp/Resources/Pages/default.aspx
3 Reference Event information at your Regional Events Analysis department **and** at http://www.nerc.com/pa/rrm/Pages/Default.aspx
4 Reference RISC Reliability Reports at http://www.nerc.com/comm/RISC/Pages/Related-Files.aspx
5 Reference Risk Elements Guide at http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Final_RiskElementsGuide_090814.pdf
6 Reference Inherent Risk Assessment Guide at http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO_Enterprise_Inherent_Risk_Assessment_Guide_20141010.pdf
7 Reference Internal Control Evaluation Guide at http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO%20Enterprise%20Internal%20Control%20Evaluation%20Guide.pdf
8 Reference NERC Compliance Monitoring and Enforcement Program at http://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix_4C_CMEP_20151104.pdf

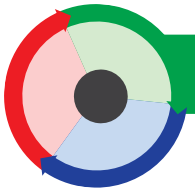


AUDITOR HANDBOOK | TABLE OF CONTENTS

<< AUDITOR HANDBOOK | INTRODUCTION >>

Note: Please click on the individual Task # if you would like to go to that specific section.

GLOSSARY | AUDITOR CHECKLIST



01-0000 | Audit Planning

Area Overview:

Audit Planning is a function of understanding a registered entity's inherent risk relative to their registered function(s) and selecting Reliability Standards and Requirements for review that will provide the greatest level of reasonable assurance that a registered entity is compliant.

Audit Planning consists of six (6) Tasks and their associated Action Items. Certain Tasks and Action Items may be performed within either the Compliance department or a designated regional group that supports the Compliance department.

The purpose of the Audit Planning Area is to understand a registered entity, define audit objectives, appropriately scope the audit, and communicate that scope to the audit team and the registered entity. A well-planned compliance audit is the basis for performing an effective audit of the registered entity.

Tasks

Task #	Task
01-0100	Audit Scoping
01-0200	Assemble and Brief the Audit Team
01-0300	Confirm Independence
01-0400	Prepare Audit Notification Packet
01-0500	Send Audit Notification Packet
01-0600	Sample and Test Agenda

P-01

Audit Planning:

Planning is the foundational activity for auditing. A well-planned audit: assures understanding of the registered entities, assesses risk, sets audit objectives, defines scope based on analysis, designs testing methodology, and anticipates audit nuances.

Auditors should be familiar with:

- ✓ Annual CMEP Implementation Plan
- ✓ Reliability Standards
- ✓ RSAWs
- ✓ Registration Functions
- ✓ Audit Risk
- ✓ Audit Scope

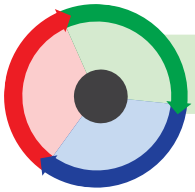
Key Documents to Complete:

- Pre-Audit Survey
- Inherent Risk Assessment
- Conflict of Interest forms
- Audit Notification Packet

Anticipated Start: When Assigned
Anticipated Finish: Audit Start Date

Guiding Documents:

- Compliance Auditor Capabilities and Competency Guide
- IIA-IPPF Standards – Code of Ethics; Standards 1100 and 1200
- GAGAS – Chapter 3 General Standards
- CMEP – Section 3.1
- ERO Enterprise Guide for Compliance Monitoring
- ERO Enterprise Guide for Internal Controls



01-0100 | Audit Planning >> Audit Scoping

01-0100

Task Overview:

Audit scoping is the determination of the Reliability Standards and Requirements that will be reviewed and tested in connection with a compliance audit. Preliminary assessment determinations are made regarding the period of time that will be tested to obtain a reasonable assurance of compliance.

The ATL shall review the Registered Entity Profile, evaluation information, Inherent Risk Assessment, and Compliance Oversight Plan.

Action Items

Action Item #	Action Item
01-0101	ATL to review the IRA and COP and finalize the audit scope

Task Highlights

The audit scoping Task is used to develop the Audit Notification Packet.

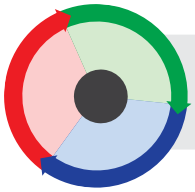
The process is complete when the three Action Items are complete and the audit scope and audit period are approved by management.

Key Documents to Complete:

- Registered entity audit scope
- Auditor Checklist: Audit Planning Checklist tasks

Task Timing:

- Audit scope must be completed prior to sending Audit Notification Letter, which is required 90 days prior to the start of audit



01-0101 | Audit Planning >> Audit Scoping >> ATL to Obtain the IRA and COP, and Finalize the Audit Scope

01-0101

Action Item:

Determine initial scope based on the current NERC Compliance Monitoring and Enforcement Plan (CMEP) Annual CMEP Implementation Plan for the audit year and other applicable Reliability Standards which were identified in the Inherent Risk Assessment and Compliance Oversight Plan.

Action Item Purpose:

The purpose of this action is to re-evaluate the registered entity's Inherent Risk Assessment (IRA) and Compliance Oversight Plan (COP) and to confirm the information is current.

An additional purpose is to review any changes to NERC Reliability Standards, bulletins, and other communications that were published after the IRA and COP were completed that may impact the audit scope.

Action Item Steps

1. *(Optional Step)* Conduct meeting with the assessment team to review and update the Registered Entity Profile and Inherent Risk Assessment.
2. Review the Registered Entity Profile, Inherent Risk Assessment, and Compliance Oversight Plan information.
3. Review with Events Analysis team for any events that have occurred since the IRA and COP were developed.
4. Meet with Enforcement to obtain an update on any Open Enforcement Activities that may impact scope.
5. Identify changes to the ERO CMEP IP that impact the selected Reliability Standards and
6. Requirements noted for scoping.
7. Review bulletins, directives, NERC communications, and other FERC, NERC, and regional guidance that will impact the selection of Reliability Standards and Requirements.
8. Adjust scope to consider risks and Reliability Standards that have been updated.
9. Identify Reliability Standards and Requirements for potential scope modification.
10. Add scoping documentation and proposed scope modification basis to workpapers.
11. Complete the Auditor Checklist Action Item.

Action Item Highlights

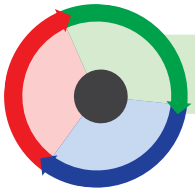
Action Owner: Audit Team Lead/Assessment Team
Action Reviewer: Not Required
Final Approver: Not Required
Process Timing:

Action Item Tips & Techniques

Regional Entities use various departments and timing regarding the development of audit scope. Follow your regional process.

Action Item References

1. CMEP – Section 3.14



01-0200 | Audit Planning >> Assemble and Brief the Audit Team

01-0200

Task Overview:

The purpose of this Task is to identify and select a team with the collective knowledge, skills, and abilities needed to perform the audit. Identified gaps that impact the audit must be resolved.

The audit team will be provided with their primary assignments and responsibilities. Communication protocol will be established for the team. The audit scoping materials and any other helpful information will be provided to the audit team. Goals, expectations, and audit timelines will be provided to the audit team. Logistical information for completing the audit will be provided to the audit team.

Action Items

Action Item #	Action Item
01-0201	Assign and document roles and responsibilities
01-0202	Establish internal project milestones, goals, and expectations
01-0203	Provide and review the audit scope and supporting materials, including prior compliance monitoring history, lessons learned, and Inherent Risk Assessment with the audit team

Task Highlights

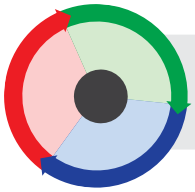
Assemble the audit team and identify team assignments, goals, and logistics. Then share the Pre-Audit Planning materials with the audit team.

Key Documents to Complete:

- Compliance Auditor assignments
- Compliance Auditor independence
- Compliance Auditor training
- Observers *(FERC/NERC/Regional management and staff)*
- Action plan to address identified gaps
- Audit team meetings and the items discussed and completed during the meetings
- Logistics for the audit team if travel is required

Task Timing:

- Varies based on Regional processes



01-0201

Action Item:

Assign and document roles and responsibilities.

Action Item Purpose:

The purpose of this action is to finalize the assignment of Compliance Auditors to the identified audit objectives and scope in preparation for communication to the audit team.

Action Item Steps

1. Document audit assignments as applicable:
   a. Alternate ATL
   b. Sub-team leads
   c. Sub-team Reliability Standard and Requirement responsibilities
   d. Sub-team member assignments per Regional Entity practice
2. Document assignments in the workpapers.
3. Complete the Auditor Checklist Action Item.

Action Item Highlights

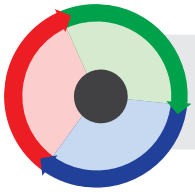
Action Owner: Audit Team Lead
Action Reviewer: Not Required
Final Approver: Not Required
Action Timing:

Action Item Tips & Techniques

Consider assigning less experienced auditors with experienced auditors for knowledge transfer and coaching.

Action Item References

1. GAGAS – Sections 3.72, 6.45 – 6.46
2. IIA-IPPF – Standards 1210 and 2030
3. CMEP – Section 3.1.5



01-0202

01-0202 | Audit Planning >> Assemble and Brief the Audit Team >> Establish Internal Project Milestones, Goals, and Expectations

Action Item:

Establish internal project milestones, goals, and expectations.

Action Item Purpose:

The purpose of this action is to establish the internal project milestones and deliverables, and define ownership and timing of activities. The purpose of this action is also for the ATL to establish goals and expectations in preparation for the audit team briefing. The audit team needs to have a clear understanding of general expectations, registered entity rules and procedures, and expected professional conduct.

Action Item Steps

1. Establish key engagement milestone dates:
   a. Initial notice and evidence request issued
   b. Compliance Auditor objections' deadline
   c. Pre-audit evidence review
   d. RSAWs/initial evidence deadline
   e. First day of the audit
   f. Final report delivered to audited entity
2. Document key milestone dates in the workpapers to share with the audit team.
3. Complete the Auditor Checklist Action Item.
4. Develop the following and prepare for discussions with the audit team:
   - Professional standards: code of conduct, managing crucial conversations, team/personal behavior.
   - General expectations: dress code, data requests, interviewing, caucus procedures, observer interaction, discussion of findings and recommendations, evidence/information handling, confidentiality, electronic device management, and non-audit activities during the audit.
   - Registered entity rules and procedures: site logistics, visitor expectations, safety, field site visits, and other known information.
5. Document the goals and expectations in the workpapers.
6. Complete the Auditor Checklist Action Item.

Action Item Highlights

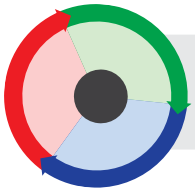
Action Owner: Audit Team Lead
Action Reviewer: Not Required
Final Approver: Not Required
Action Timing:

Action Item Tips & Techniques

1. Consider developing a master audit schedule on a yearly basis. Individual audit schedules should be reconciled against the master schedule.
2. Multi-Region audit key milestone dates must be established before any other audits are planned.
3. Audit Management must be notified if key milestone dates are at risk or when conflicts cannot be resolved.
4. Goal and expectation detail level should be the same for each audit.
5. The ATL should review the pre-audit survey and ensure the entity PCC has received the audit team's specific requirements.
6. Determine necessary identification and documentation required for facility access *(e.g., passports, visas, government issued ID)*.
7. Auditors should familiarize themselves with professional standards and their Regional Entity's code of conduct.

Action Item References

1. GAGAS – Sections 6.51, 6.53, and 6.54
2. IIA-IPPF – Standards 1120, 1130, 1200, and 2340
3. CMEP – Sections 3.1.1, 3.1.2, and 3.1.5.3 *(necessary only for observers)*



01-0203 | Audit Planning >> Assemble and Brief the Audit Team >> Team Member Briefing

01-0203

Action Item:

Provide and review the audit scope and supporting materials, including prior monitoring history, lessons learned, and the Inherent Risk Assessment with the audit team.

Action Item Purpose:

The purpose of this action is to provide the audit team with the communication protocol, audit objectives, audit scope, Inherent Risk Assessment, test plans, and audit team assignments. Additionally, the audit team will discuss the registered entity's compliance history, including prior testing and results, with emphasis on past compliance issues, corrective actions, and Reliability Standards for the registered entity that have not been included in any recent compliance monitoring method.

Action Item Steps

1. Conduct meeting with the audit team and observers to communicate the following:
   - Audit team roles and responsibilities
   - Communication protocol
   - Project milestones
   - Goals and expectations
   - Audit objectives
   - Inherent Risk Assessment
   - Audit scoping documents
   - Audit travel and logistics
2. Review culture of compliance, areas of concern, and recommendations from previous compliance monitoring and enforcement activities.
3. Review professional standards, ethical principles, and rules of conduct with the audit team.
4. The audit team needs to review and understand:
   a. Applicable implementation plans and transition plans
   b. For CIP engagements: applicable Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities (IPFNICCAANRE)
5. Document the audit team briefing in the workpapers.
6. Complete the Auditor Checklist Action Item.

Action Item Highlights

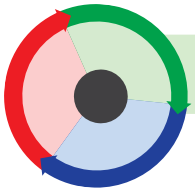
Action Owner: Audit Team Lead
Action Reviewer: Not Required
Final Approver: Not Required
Action Timing:

Action Item Tips & Techniques

The audit team needs to have a thorough understanding of the registered entity.

Action Item References

1. GAGAS – Section 6.36
2. IPFNICCAANRE



01-0300 | Audit Planning >> Confirm Independence

01-0300

Task Overview:

Confirming independence verifies the Compliance Auditors, including Regional Entity staff and contractors, and third-party team member have no conflicts with the registered entity being audited. This is to ensure the independence and objectivity of the audit team.

Action Items

Action Item #	Action Item
01-0301	Confirm independence and address conflicts of interest for each Compliance Auditor, consultant, and third-party team member

Task Highlights

This is to confirm the independence of the audit team from the registered entity being audited.

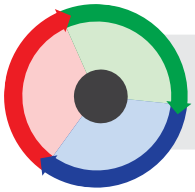
Key Documents to Complete:

- Conflict of Interest forms, Confidentiality Agreements, or other acknowledgments for all Compliance Auditors, including contractors
- The process is complete when the forms and verification are documented in the workpapers

Process Timing:

- 30 days prior to start of audit

This step must be completed prior to sending the audit notification packet to the registered entity's PCC.



01-0301 | Audit Planning >> Confirm Independence >> Confirm Independence

01-0301

Action Item:

Confirm independence and address conflicts of interest for each Compliance Auditor, consultant, and third-party team member.

Action Item Purpose:

- Ensure the Compliance Auditors, non-Regional Entity staff, including contractors, observers, and other audit participants are and remain independent in accordance with the NERC Rules of Procedure (ROP), professional standards, and Regional Entity guidance, at the time of and during the audit. Independence includes the ability to maintain objectivity throughout the course of the audit.
- Verify that employee members of the audit team have completed their annual disclosures regarding independence and conflicts of interest. Audit management should review concepts of independence, objectivity, and conflicts with audit team members on a routine basis.
- Verify that Compliance Auditors are compliant with requirements regarding NERC training, Regional Entity training, and other mandatory requirements for performing audit activities.

Action Item Steps

1. Verify the existence of a completed Conflict of Interest and Confidentiality Agreement form for each Compliance Auditor, contractors, observers, and other audit attendees as needed.
2. Notify Audit Management and modify the audit team accordingly to resolve any conflicts.
3. Remind audit team and non-Regional Entity staff team members to immediately advise Audit Management if any conflicts of interest arise between the time of this verification and the completion of the audit.
4. Per Regional Entity policies, verify that a current Personnel Risk Assessment exists for each non-Regional audit attendee.
5. Document the independence verification in the workpapers.
6. Review the employee and contractor roster to verify that Compliance Auditors meet NERC and Regional requirements for performing audit activities.
7. Review the roster on a routine basis to verify qualifications.
8. Complete the Auditor Checklist Action Item.

Action Item Highlights

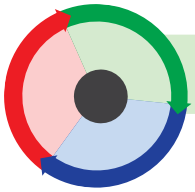
Action Owner: Audit Team Lead/Audit Management
Action Reviewer: Not Required
Final Approver: Not Required
Action Timing:

Action Item Tips & Techniques

1. Understand the expectations of independence.
2. Review previous Compliance Auditor and non-Regional Entity audit attendee participation on compliance monitoring activities.
3. The ATL must be mindful of independence at the functional registration, subsidiary, and parent company levels.
4. Compliance Auditors and non-Regional Entity audit attendees must comply with Regional Policies regarding acceptance of gifts.
5. Auditors should be familiar with professional standards, ethical principles, and rules of conduct.
6. Conflict of interest form and confidentiality agreements should be completed at the beginning of each year.
7. Conflict of interest forms should be reviewed prior to sending the audit detail letter.
8. Completion of conflict of interest forms is an opportunity to familiarize auditors with regional and NERC policies on independence.
9. Employees should be aware of policies related to gifts, meals, and entertainment that may impact independence.
10. Questions regarding conflicts of interest and independence should be addressed with management and when necessary the Legal department.

Action Item References

1. GAGAS – Sections 1.19, 1.24, 3.01-3.32, and 3.13 – 3.19
2. IIA-IPPF –Code of Ethics, Standards 1100, 1120, and 1130
3. CMEP – Section 3.1.5.2
4. Periodic NERC Training announcements
5. Compliance Auditor Capabilities and Compliance



01-0400 | Audit Planning >> Prepare Audit Notification Packet

01-0400

Task Overview:

The purpose of this Task is to assemble the information derived from the prior Tasks and actions to create the packet of information sent to the registered entity to start the audit engagement. The Audit Notification Packet will include the materials outlining the audit dates, milestones, audit team, contact information, audit scope, audit period, and the initial data request.

Action Items

Action Item #	Action Item
01-0401	Audit Notification Packet Preparation
01-0402	Audit Notification Packet Review

Task Highlights

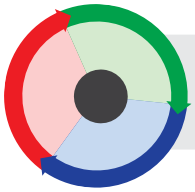
Prepare the Audit Notification Packet and have it reviewed before sending it to the registered entity.

Key Documents to Complete:

- Region specific documents as appropriate

Process Timing:

- 90 - 120 days



01-0401 | Audit Planning >> Prepare Audit Notification Packet >> Prepare Preliminary Audit Notification Packet

01-0401

Action Item:

Prepare a preliminary Audit Notification Packet/request list to be sent out to the registered entity that includes the following:

- Requests for supporting documentation for the purposes of testing the Reliability Standards.
- Nondisclosure or Confidentiality Agreements for audit team members.
- Pre-Audit and Compliance Surveys to be completed by the registered entity.

Action Item Purpose:

The purpose of this action is to prepare the Audit Notification Packet used to formally notify the registered entity about the scheduled audit.

Action Item Steps

1. Prepare and assemble the following required documents:
   a. Audit notification letter
   b. Compliance Auditor biographies, Confidentiality Agreements, codes of conduct, and conflict of interest communication
   c. Initial evidence request with submission deadlines
      i. To include the CIP Version 5 Evidence Request and User Guide
   d. NERC Compliance Audit Certification:
      i. Compliance Audit Information Certification Letter
      ii. Attachment B to the Compliance Audit Information Certification Letter in Word format
   e. Nondisclosure/Confidentiality Agreements, Conflict of Interest, etc. for all non-government regulatory observers
2. Prepare and assemble Regional Entity-specific Audit Notification Packet Documents.
3. Ensure all observers and NERC are included on distribution lists.
4. Submit Notification Packet for review per Regional Entity practice.
5. Complete the Auditor Checklist Action Item.

Action Item Highlights

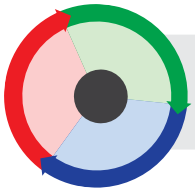
Action Owner: Audit Team Lead/Audit Team Support
Action Reviewer: Not Required
Final Approver: Not Required
Action Timing:

Action Item Tips & Techniques

1. Use of a Microsoft Word Mail Merge template helps populate the correct registered entity information.
2. Review the results of 01-0101 for audit scope.
3. New preparers should familiarize themselves with prior audit notifications.
4. Keep observers copied on communications.
5. Non-disclosure/Confidentiality agreements not required for government regulatory observers *(e.g., FERC, Canadian provincial regulators)*.

Action Item References

1. CMEP – Sections 3.1.1, 3.1.4, and 3.1.5



01-0402 | Audit Planning >> Prepare Audit Notification Packet >> Perform Review of the Audit Notification Packet

01-0402

Action Item:

Perform review of the Audit Notification Packet *(person other than the preparer)*.

Action Item Purpose:

The purpose of this action is a person other than the preparer to perform a final review of the Audit Notification Packet.

Action Item Steps

1. The assigned reviewer *(person other than the preparer)*:
   a. Validates the accuracy and completeness
   b. Provides comments/corrections as necessary
   c. Return any questions are to be answered or corrections to be made to the preparer for action
2. Approve the Audit Notification Packet for distribution once all questions and comments are resolved.
3. Maintain an approved copy of the notification packet in the workpapers.
4. Complete the Auditor Checklist Action Item.

Action Item Highlights

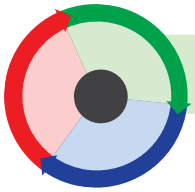
Action Owner: Audit Team Lead/Audit Team Support
Action Reviewer: Not Required
Final Approver: Audit Management
Action Timing:

Action Item Tips & Techniques

1. Special attention should be given to:
   a. Dates of the engagement
   b. Deadlines/milestones
   c. Audit team information
   d. Contact information
   e. Registered entity name, NCR number, and registered functions
   f. Audit scope, audit period, and Reliability Standard version
   g. Initial data requests
2. New reviewers should familiarize themselves with prior audit notifications.

Action Item References

1. GAGAS – Sections 6.53 – 6.55
2. CMEP – Sections 3.1.1, 3.1.4, and 3.1.5



01-0500 | Audit Planning >> Send Audit Notification Packet

01-0500

Task Overview:

The purpose of this Task is to alert and inform the registered entity of the pending audit engagement. The Audit Notification Packet must be comprehensive and provide the required material to the registered entity.

Action Items

Action Item #	Action Item
01-0501	Registered Entity Notification
01-0502	Registered Entity Coordination Meeting

Task Highlights

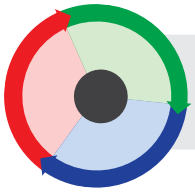
The Task is complete when it is confirmed the registered entity has received the Audit Notification Packet and the pre-audit meeting has been conducted. The goal of this Task is to set the audit up for success for both the Compliance Auditors and registered entity.

Key Documents to Complete:

- Audit Notification Packet
- Delivery confirmation

Task Timing:

- 90 days prior to start of audit



01-0501 | Audit Planning >> Send Audit Notification Packet >> Registered Entity Notification

01-0501

Action Item:

Communicate in writing with the registered entity being audited to cover objectives, audit scope, expectations, logistics, and timing of the audit.

Action Item Purpose:

The purpose of this action is to send the Audit Notification Packet to communicate the audit objectives, audit scope, expectations, general audit logistics, and timing of the audit in writing to the registered entity. The action is completed to verify the registered entity is aware of the expectations for these key areas of the audit.

Action Item Steps

1. Transmit Audit Notification Packet to registered entity per Regional Entity practice with receipt confirmation requested.
2. Follow up with registered entity PCC if no receipt confirmation is received within one working day.
3. Document the transmission of the Audit Notification Packet and receipt confirmation in the workpapers.
4. Complete the Auditor Checklist Action Item.

Action Item Highlights

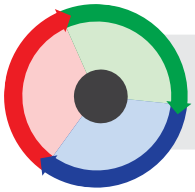
Action Owner: Audit Team Lead/Audit Team Support
Action Reviewer: Not Required
Final Approver: Not Required
Action Timing:

Action Item Tips & Techniques

1. Set the Delivery and Read Receipt check boxes when transmitting the audit notification packet by email.
2. If transmitted by email, request the registered entity PCC reply by email confirming receipt.

Action Item References

1. GAGAS – Sections 6.47 – 6.49
2. CMEP – Sections 3.1.1, 3.1.4, and 3.1.5



01-0502 | Audit Planning >> Send Audit Notification Packet >> Registered Entity Coordination Meeting

01-0502

Action Item:

Coordinate a pre-audit meeting with key personnel within the registered entity to discuss the audit, expectations, and any questions related to the information included in the initial Audit Notification Packet.

Action Item Purpose:

The purpose of this action is to schedule and conduct an initial coordination meeting between the ATL and the registered entity.

Action Item Steps

1. Schedule the coordination meeting.
2. Conduct the coordination meeting to discuss the following recommended topics:
   a. Audit scope, schedule, and key dates
   b. General information
   c. Evidence request and handling
   d. Data request expectations and deadlines
   e. PPE requirements
   f. Questions or comments on the Audit Notification Packet
3. Follow up on any questions or comments that could not be addressed during the coordination meeting.
4. Document the meeting in the workpapers.
5. Complete the Auditor Checklist Action Item.

Action Item Highlights

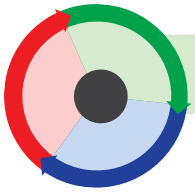
Action Owner: Audit Team Lead
Action Reviewer: Not Required
Final Approver: Not Required
Action Timing:

Action Item Tips & Techniques

1. The coordination meeting may be conducted by phone or webinar.
2. The ATL makes sure the appropriate Compliance Auditors and observers attend the coordination meeting.
3. The coordination meeting should be conducted within one week of confirmation of receipt of the Audit Notification Packet.

Action Item References

1. GAGAS – Sections 6.47 – 6.49
2. CMEP – Sections 3.1.1, 3.1.4, and 3.1.5



01-0600 | Audit Planning >> Sample and Test Agenda

01-0600

Task Overview:

The purpose of this Task is to define and document an audit sampling approach and sampled evidence requests. It is also to communicate the sampled evidence request to the registered entity. Sampling methodology must comply with ERO Enterprise Sampling Guide and other generally accepted auditing practices.

Action Items

Action Item #	Action Item
01-0601	Utilize NERC approved NERC Sampling Methodology Guidelines and Criteria to develop samples to test the in-scope requirements, and submit the samples to the entity

Task Highlights

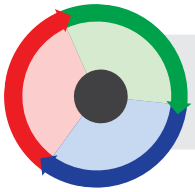
Requests for evidence to be sampled are submitted, received, and reviewed as many times as necessary to acquire sufficient evidence for evaluation.

Key Documents to Complete:

- ERO Enterprise Sampling Guide
- Regional template or document for the sample request

Process Timing:

- Throughout the audit Regional template or document for the sample request



01-0601 | Audit Planning >> Sample and Test Agenda >> Sample Determination and Testing

01-0601

Action Item:

Utilize NERC approved ERO Enterprise Sampling Guide to develop samples to test the in-scope requirements, and submit the samples to the entity.

Action Item Purpose:

The purpose of this action item is to use recommended methodologies that have been developed for the testing of Reliability Standards and Requirements and to create the sample evidence request and provide the sample evidence request to the registered entity. If the Audit Team deviates from the suggested methodology, the methodology used along with the rationale for the deviation needs to be documented to support the testing and results. While coordination with the registered entity may be necessary to review the sample evidence request.

Action Item Steps

1. Review the ERO Enterprise Sampling Guide to develop the sampling selection based on data characteristics.
2. For CIP Audits, utilize the CIP Version 5 Evidence Request if appropriate for the scope of the audit engagement.
3. Review the data population and identify the audit samples.
4. The audit team meets with its ATL to discuss registered entity involvement in events or any other special activities for judgmental inclusion or exclusion from audit samples.
5. The ATL confirms with the Auditor that ERO Enterprise Sampling Guide is used for all sampling performed for the audit or that deviations *(alternate method used and rationale for the deviation)* have been documented and approved.
6. The ATL assures the audit team followed the steps to perform the sampling, along with the actual samples selected.
7. Document the sample determination and the test plans in the workpapers.
8. Transmit the request for sample evidence selected for testing to the registered entity. Request a confirmation of receipt from the registered entity PCC.
9. Coordinate and conduct conference calls as needed with the registered entity PCC to confirm the evidence request and answer any questions regarding the sample selection.
10. Transmit additional evidence requests as required for specific testing.
11. Document the request for sample evidence and associated conversations in the workpapers.
12. Complete the Auditor Checklist Action Item.

Action Item Highlights

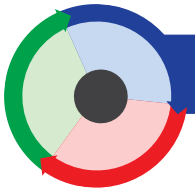
Action Owner: Audit Team Lead
Action Reviewer: Not Required
Final Approver: Not Required
Action Timing: Occurs throughout the audit

Action Item Tips & Techniques

1. Use automated sampling software *(e.g., RAT-STATS)* if appropriate.
2. Use Microsoft Excel for selecting a random sample if appropriate.
3. Verify the source population data is in the requested format.
4. Utilize a template or document for the sample request *(e.g., Excel spreadsheet)*.
5. Consider registered entity-specific control design when developing test plans.
6. Review KRSSC sampling guide for PRC-005 http://www.nerc.com/files/PRC-005-1%20 kRSSC%20 Final%20Report-%2009142011.pdf.

Action Item References

1. GAGAS – Sections 6.64 – 6.66
2. IIA-IPPF – Standards 2320, 2330, and Practice Advisory 2320-3
3. RAT-STATS
4. ERO Sampling Guide
5. CIP Version 5 Evidence Request and User Guide



02-0000 | Audit Fieldwork

02-0000

Area Overview:

Compliance Auditors must use information that is sufficient and appropriate to support findings and conclusions developed through the course of the audit cycle.

Audit Fieldwork consists of eleven (11) Tasks and their associated Action Items. Tasks and Actions in the Audit Fieldwork Area are performed by an auditor both in the office and in field locations as needed to meet the nature and extent of testing required. Compliance Auditors are expected to maintain complete workpapers. Workpapers must support the selection and review of evidence as well as the conclusions that are drawn in a manner that would permit an informed person to reach the same conclusion.

The purpose of Audit Fieldwork is to build on the activities performed in planning and carrying out activities to obtain, review, assess, test, and document the information and data that supports the audit objectives. It is the Compliance Auditor's responsibility to appropriately consider audit risk, make determinations of significance, and obtain reasonable assurance of compliance with Reliability Standards.

Tasks

Task #	Task
02-0100	Preliminary Documentation Review
02-0200	Additional Documentation Request
02-0300	Final Planning Meeting
02-0400	Conduct Opening Presentation
02-0500	SME Interviews
02-0600	Documenting Results
02-0700	Document Findings
02-0800	Audit Team Debrief
02-0900	Status Briefings
02-1000	Audit Team Conclusions
02-1100	Exit Briefing

P-02

Audit Fieldwork:

Audit Fieldwork is a team effort that is directed by the ATL. It consists of obtaining, reviewing, assessing, and testing documentation provided by the registered entity to determine compliance with Reliability Standards. Ongoing communication with the PCC and designated registered entity personnel helps ensure the audit objectives are understood and completed.

Auditors should be familiar with:

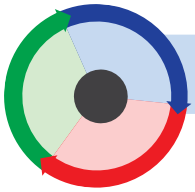
- ✓ Reliability Standards
- ✓ Audit Risk
- ✓ Significance
- ✓ Reasonable Assurance
- ✓ Interviewing and Documentation
- ✓ Record Management
- ✓ Presentation Skills
- ✓ Reliability Standards Audit Worksheet
- ✓ Design and Completion of Audit Testing
- ✓ Sampling
- ✓ Quality of Evidence
- ✓ Terms and Acronyms

Key Documents to Complete:

- RSAW
- Interview and conversation documentation
- Evidence Requests
- Presentations *(open, status, and exit)*
- NERC feedback form

Anticipated Start: 90 days following the audit notice

Anticipated Finish: Final day of the audit *(exit presentation)*



02-0100 | Audit Fieldwork >> Preliminary Documentation Review

02-0100

Task Overview:

The purpose of this Task is for the Audit Team to perform a pre-audit evidence review of the information and data submission from the registered entity. The Audit Team will review the evidence for reliability, accuracy, validity, and sufficiency. This review will be documented in the workpapers and form the basis for determining if further documentation will be required.

Action Items

Action Item #	Action Item
02-0101	Review the completeness, accuracy, and validity of the supporting documentation requested. Draft follow up inquiries and procedures, identify audit team conclusions, and document gaps. Determine whether additional documentation is required to satisfy the audit objectives

Task Highlights

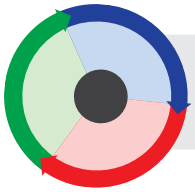
The Task is considered complete when the initial information and data submission from the registered entity has been reviewed and documented within the RSAWs.

Key Documents to Complete:

- Documentation within the workpapers of the initial review
- Documentation of additional evidence requirements and follow-up questions in the workpapers

Process Timing:

- Typically 30 days prior to start of the audit



02-0101 | Audit Fieldwork >> Preliminary Documentation Review >> Pre-Audit Evidence Review

02-0101

Action Item:

Review the completeness, accuracy, and validity of the supporting documentation requested. Draft follow up inquiries and procedures, identify audit team conclusions, and document gaps. Determine whether additional documentation is required to satisfy the audit objectives.

Action Item Purpose:

The purpose of this action is to review information and data provided from the registered entity. The audit team performs an assessment of the information and data to make a determination of sufficiency with regards to validity of the information and appropriateness of requested format, and to reflect the period of time requested. The audit team will evaluate the information and data to perform initial test steps for determinations, select samples for supporting documentation, request additional information and data for insufficient data, and prepare for on-site testing.

The audit team will sort the evidence into categories:

- Additional information required to perform testing, or
- Documentation necessary to address insufficient or deficient evidence in support of compliance with the Reliability Standard.

Action Item Steps

1. For each Reliability Standard and Requirement in scope, perform the following:
   a. Assess and validate the submitted evidence to ensure it is sufficient and appropriate:
      i. Evidence is in the requested *(or an acceptable)* format
      ii. Evidence is applicable to the Reliability Standard and Requirement
      iii. Evidence covers the appropriate time period
   b. For evidence found to be sufficient and appropriate, evaluate it for completeness:
      i. Evidence is sufficient and appropriate for developing audit team conclusions and sample evidence requests.
      ii. Evidence is not sufficient and appropriate to make audit team conclusions; additional evidence or clarification is required.
   c. If evidence is sufficient and appropriate to demonstrate a reasonable assurance of compliance, determine "No Finding." Proceed to Action Item 02-0801.
2. Determine the reason additional documentation is required:
   a. Evidence is deficient *(e.g., wrong format, wrong time period, not relevant)*. Proceed to Action Item 02-0201.
   b. Evidence is insufficient to make a preliminary determination of compliance. Proceed to Action Item 02-0201.
   c. Evidence is to be sampled from previously provided evidence sets. Proceed to Action Item 02-0202.
3. Document the evaluation results within the workpapers.
4. Complete the Auditor Checklist Action Item.

Action Item Highlights

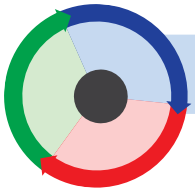
Action Owner: Audit Team Lead
Action Reviewer: Not Required
Final Approver: Not Required
Action Timing:

Action Item Tips & Techniques

1. Pre-evidence review methods:
   a. Inquiry
   b. Observation
   c. Physical Examination
   d. Documentation Review
   e. Reperformance
   f. Confirmation
2. Available evidence may be limited by data retention requirements of the Reliability Standard or NERC guidance.
3. Evidence of approval may be a physical signature, electronic signature/mark, or workflow process log.

Action Item References

1. GAGAS – Sections 6.60 – 6.72
2. IIA-IPPF – Standards 2120, 2130, and 2320
3. CMEP – Section 3.1.1
4. NERC presentation forms and quality of evidence
5. NERC Compliance Process Bulletin #2009-005
6. IIA-IPPF – Standards 2310 – 2330



02-0200 | Audit Fieldwork >> Additional Documentation Request

02-0200

Task Overview:

The purpose of this Task is for the audit team to perform preliminary reviews of additional evidence needs and to provide the registered entity PCC with those additional evidence requests. The audit team documents their findings in a sufficient manner that will support testing conclusions. The audit team is responsible for assuring the registered entity PCC understands the nature and rationale for the evidence requests.

Action Items

Action Item #	Action Item
02-0201	Evidence Evaluation
02-0202	Requests for Additional Evidence

Task Highlights

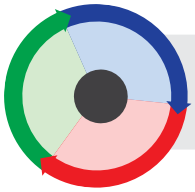
The Task is considered complete when additional evidence requests have been provided to the registered entity PCC.

Key Documents to Complete:

- Evidence requests finalized and transmitted to the registered entity PCC
- Interview questions noted in the workpapers
- Evidence requests and supporting correspondence documented in the workpapers

Process Timing:

- From initial evidence submittal to close of audit



02-0201

02-0201 | Audit Fieldwork >> Additional Documentation Request >> Evidence Evaluation

Action Item:

Evaluate whether the lack of supporting documentation is due to deficiencies or other program weaknesses, and whether the lack of documentation could be the basis for findings.

Action Item Purpose:

The purpose of this action is to perform an additional assessment of the submitted evidence that has been identified as insufficient or deficient to adequately support compliance with the Reliability Standards being tested. The audit team develops follow-up questions and additional requests for evidence to address the insufficiency or deficiency.

Action Item Steps

1. Evidence is insufficient to be able to develop a conclusion:
   a. Prepare to discuss evidence concerns with the registered entity PCC
   b. Draft additional evidence request(s) to resolve the insufficiency
2. Evidence is deficient:
   a. Evidence submitted to date is suggestive of a finding
   b. Prepare to discuss evidence concerns with the registered entity PCC
   c. Draft additional evidence request(s) to resolve or confirm the deficiency
3. Document the evaluation and preparation steps in the workpapers.
4. Complete the Auditor Checklist Action Item.

Action Item Highlights

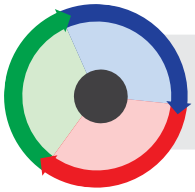
Action Owner: Audit Team Lead
Action Reviewer: Audit Management
Final Approver: Audit Management
Action Timing:

Action Item Tips & Techniques

1. Ask the registered entity's PCC if they refer to requested documentation as something different and give examples.
2. Consider and suggest alternative sources of evidence.
3. Even if the SME states that evidence is not available, request the evidence and require a written response.
4. Understand what information or data is incomplete in order to help develop better future evidence requests.
5. In some situations meeting with the SMEs *(whether over the phone or in person)* gives the audit team an opportunity to confirm if a gap exists in documentation or if additional documentation could be requested from the registered entity.

Action Item References

1. GAGAS – Sections 6.60 – 6.72
2. IIA-IPPF – Standards 2310 – 2330
3. CMEP – Section 3.1.1



02-0202 | Audit Fieldwork >> Additional Documentation Request >> Requests for Additional Evidence

02-0202

Action Item:

Send subsequent sample and data requests when required.

Action Item Purpose:

The purpose of this action is to assemble all additional evidence requests and communicate with the registered entity PCC. The audit team may develop questions associated with the additional evidence needs.

Action Item Steps

1. For evidence to be sampled, determine the sample set to be requested.
2. Send additional evidence requests to the registered entity PCC.
3. Coordinate with the registered entity PCC to determine if a follow-up conference call is desired.
4. Schedule and conduct follow-up conference call if requested by the registered entity PCC.
5. Document the evidence requests and supporting correspondence in the workpapers.
6. Complete the Auditor Checklist Action Item.

Action Item Highlights

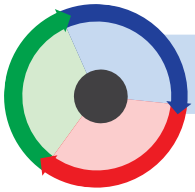
Action Owner: Audit Team Lead
Action Reviewer: Not Required
Final Approver: Not Required
Action Timing:

Action Item Tips & Techniques

1. Understand what information is incomplete in order to help develop better evidence requests.
2. Review ERO Enterprise Sampling Guide.
3. Capture potential interview questions in the workpapers as they are developed.
4. If the PCC requests, the evidence requests may be copied to additional registered entity staff.

Action Item References

1. GAGAS – Sections 6.60 – 6.72
2. IIA-IPPF – Standards 2310 – 2330
3. CMEP – Section 3.1.1



02-0300 | Audit Fieldwork >> Final Planning Meeting

02-0300

Task Overview:

The purpose of this Task is to perform final preparatory actions before the on-site portion of the Audit Fieldwork. The ATL schedules and conducts a meeting with the registered entity PCC to review the audit agenda, answer any final questions, and make any final arrangements.

Action Items

Action Item #	Action Item
03-0101	Schedule and conduct a final planning meeting to discuss expectations, milestones, agenda, status communication protocol, and additional preparatory activities

Task Highlights

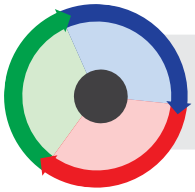
The Task is complete when the final planning meeting is conducted, all discussion items have been reviewed, and the audit agenda is finalized with the PCC.

Key Documents to Complete:

- Final audit agenda and logistics

Task Timing:

- Varies based on Regional processes



02-0301 | Audit Fieldwork >> Final Planning Meeting >> Schedule Final Planning Meeting

02-0301

Action Item:

Schedule and conduct a final planning meeting to discuss expectations, milestones, agenda, status communication protocol, and additional preparatory activities.

Action Item Purpose:

The purpose of the action is to develop the agenda with the PCC, to schedule the final planning meeting so the ATL and necessary audit team members can meet with the registered entity's contacts, and to conduct the scheduled final planning meeting to finalize the audit agenda, and schedule SME interviews.

Action Item Steps

1. Contact the PCC to establish the agenda and date of the final planning meeting.
2. Place date and time on calendar.
3. Prepare a draft audit agenda.
4. Set up dial-in numbers and/or webinar.
5. Notify audit team of the meeting and if they are needed for the meeting.
6. Send a copy of the draft agenda to the PCC and the audit team.
7. Conduct the final planning meeting with the PCC.
8. Finalize the audit agenda.
9. Finalize audit logistics.
10. Answer any questions or concerns.
11. Confirm with the PCC that the information has been adequately covered and all questions have been addressed.
12. Document the conversation and place in the workpapers.
13. Document the completion of the Action Item in the workpapers.
14. Complete the Auditor Checklist Action Item.

Action Item Highlights

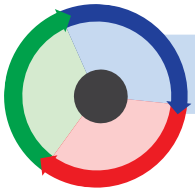
Action Owner: Audit Team Lead
Action Reviewer: Not Required
Final Approver: Not Required
Action Timing:

Action Item Tips & Techniques

1. Consider time zones for scheduling meetings.
2. Reconfirm with the PCC the date and time of the scheduled meeting.
3. Discussion items should include:
   a. Documents required for facility access
   b. Verify lunch plans and communicate the audit team is responsible for paying for their lunch
   c. Understand parking and other logistical needs.
   d. Audit evidence handling and submittals

Action Item References

1. GAGAS – Sections 6.47



02-0400 | Audit Fieldwork >> Conduct Opening Presentation

02-0400

Task Overview:

The objective of this Task is to deliver the opening presentation to the registered entity's designated personnel and provide them with opportunities to ask questions regarding the audit process. This also provides the registered entity with an opportunity to discuss their organizational culture of compliance, and additional pertinent information that will impact the audit.

The opening presentation sets expectations, timelines, and objectives of the audit engagement.

Action Items

Action Item #	Action Item
02-0401	Conduct the opening presentation meeting to reconfirm expectations, milestones, and status communication protocol

Task Highlights

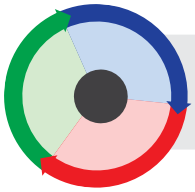
This Task is considered complete when the ATL creates the opening presentation and delivers it to the registered entity.

Key Documents to Complete:

- Regional opening presentation
- Copy of the registered entity opening presentation

Task Timing:

- First day of audit



02-0401 | Audit Fieldwork >> Conduct Opening Presentation >> Opening Presentation

02-0401

Action Item:

Conduct the opening presentation meeting to reconfirm expectations, milestones, and status communication protocol.

Action Item Purpose:

The purpose of this action is to meet with the registered entity's PCC and designated attendees at the beginning of Audit Fieldwork. The ATL coordinates the opening presentation with the PCC.

Action Item Steps

1. Develop an opening presentation that covers the following items:
   a. CEA program overview
   b. Audit timing
   c. Audit objectives
   d. Audit scope and what will be tested for the audit
   e. Identify the audit team
   f. Establish registered entity expectations for data requests, timing, discussions, and demonstration of compliance
   g. Schedule of activities, including interviews
   h. Protocol for conducting meetings and caucuses
   i. How audit conclusions will be reviewed
   j. Internal Controls
2. The ATL schedules the opening presentation meeting with the PCC.
3. Deliver the opening presentation and answer any questions.
4. Allow time for the registered entity personnel to present to the audit team.
5. Document the meeting materials and notes in the workpapers.
6. Complete the Auditor Checklist Action Item.

Action Item Highlights

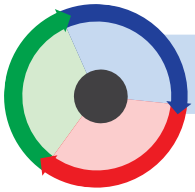
Action Owner: Audit Team Lead
Action Reviewer: Not Required
Final Approver: Not Required
Action Timing:

Action Item Tips & Techniques

1. Utilize the Regional Entity's PowerPoint templates for standardization and efficiency.
2. Delete any redundant or non-applicable information in the presentations.
3. The registered entity should conduct a facility orientation and safety review.
4. Try to limit the opening presentations to approximately 30 minutes each.
5. The ATL should provide opportunities for auditors to present.
6. In addition to emailing the presentation, a thumb drive is recommended as a back-up. Only use your region approved back-up medium.
7. ATL's should practice the delivering the presentation and work with team members as appropriate.

Action Item References

1. GAGAS – Sections 6.47 – 6.51



02-0500 | Audit Fieldwork >> SME Interviews

02-0500

Task Overview:

The purpose of the Task is to schedule SME interviews, conduct interviews, obtain sufficient evidence, and document supporting conclusions within the workpapers.

Action Items

Action Item #	Action Item
02-0501	Conduct interviews with the registered entity. The following should be considered during the discussions

Task Highlights

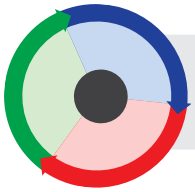
The Task is considered complete when the audit team has validated and documented outstanding audit questions with the appropriate SMEs.

Key Documents to Complete:

- Conversation and interview documents

Task Timing:

- During the audit



02-0501

Action Item:

Conduct interviews with the registered entity. The following should be considered during the discussions:

- Understand the policies, procedures, and processes by which the registered entity complies with the relevant Reliability Standards
- Understand how often the procedures/processes are performed *(i.e., frequency)*
- Confirm who owns and performs each policy/procedure/process
- Assess the competency *(e.g., training, certifications, background)* of the SME or compliance contact responsible for the policy/procedure/process
- Understand interview issue/failure escalation process
- Document conversations in workpapers

Action Item Purpose:

The purpose of this action is to provide guidance on conducting interviews with registered entity's SMEs. The ATL works with the registered entity PCC to schedule the necessary meeting(s) with the appropriate SMEs to validate any outstanding questions.

Action Item Steps

1. Interview questions are prepared by the audit team in advance for all SME meetings.
2. Additional questions may be developed during the course of the interview.
3. If an issue of noncompliance does exist, then conduct meetings to discuss the facts and circumstances surrounding the noncompliance issue.
4. Conduct interviews to verify (1) that Compliance Auditors understand the facts and circumstances and (2) to give the registered entity an opportunity to provide additional documentation supporting their compliance.
5. Seek additional SMEs as necessary or refer interview issues to the PCC for resolution.
6. Document all conversations in workpapers.
7. Complete the Auditor Checklist Action Item.

Action Item Highlights

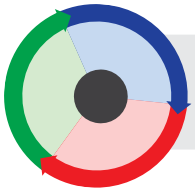
Action Owner: Audit Team Lead
Action Reviewer: Not Required
Final Approver: Not Required
Action Timing: During the audit

Action Item Tips & Techniques

1. Conflicts in the operation of the business take priority over conducting the interview.
2. Interviews can be performed either on-site with the registered entity SMEs, over the phone, or via webinar.
3. The Compliance Auditor sets the appropriate tone *(i.e., professional and conversational, not personal).*

Action Item References

1. GAGAS – Sections 6.61 – 6.62 and 6.79 – 6.83



02-0502 | Audit Fieldwork >> SME Interviews >> Obtain an Understanding of Internal Controls

02-0502

Action Item:

Obtain an understanding of internal controls related to the audit scope.

Action Item Purpose:

As part of the audit, the team should obtain an understanding of internal controls related to the scope of work performed during compliance monitoring activities. The understanding of internal controls can inform future monitoring and the Compliance Oversight Plan (COP). After reviewing internal controls, the audit team can make decisions around the effectiveness of the design and implementation that may:

- Change the nature, extent, and timing of compliance testing during fieldwork or future fieldwork
- Identify industry best practices, areas of concern, or recommendations
- Refine the registered entity's COP and future compliance monitoring

Action Item Steps

1. Review the registered entity's internal controls *(as applicable)*.
2. The Audit Team's review of internal controls can be done through:
   - Inquiries,
   - Observations,
   - Inspection of documents and records,
   - Review of other CEA staff reports, or direct tests.
3. Document the results of the review.
4. Complete the Auditor Checklist Action Item.

Action Item Highlights

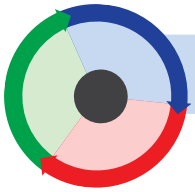
Action Owner: Audit Team Lead
Action Reviewer: Not Required
Final Approver: Not Required
Action Timing: During the audit

Action Item Tips & Techniques

1. The CEA's understanding of internal controls during CMEP activities allow the CEA to make better informed decisions around compliance and the registered entity's ability to sustain compliance and build reliability excellence.
2. The nature and extent of procedures CEA staff perform to obtain an understanding of internal control may vary based on compliance monitoring objectives, inherent risk, known or potential internal control deficiencies, and the CEA staff's knowledge about internal controls gained in prior compliance monitoring activities.

Action Item References

1. ERO Enterprise Guide for Compliance Monitoring *(current version)*.
2. ERO Enterprise Guide for Internal Controls, section 1.2



02-0600 | Audit Fieldwork >> Documenting Results

02-0600

Task Overview:

All testing approaches and results are documented within the appropriate testing document. The results of testing are communicated to the ATL and when necessary to Audit Management.

Action Items

Action Item #	Action Item
02-0601	Update auditor workpapers based upon work performed by the audit team, including sample testing

Task Highlights

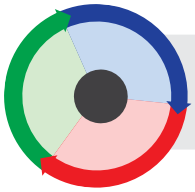
The Task is considered complete when the testing results with supporting evidence have been documented, audit team conclusions have been vetted, and the ATL has reviewed the conclusions with the audit team.

Key Documents to Complete:

- Audit results are documented within workpapers

Task Timing:

- During audit testing



02-0601 | Audit Fieldwork >> Documenting Results >> Review and Documentation of Audit Work

02-0601

Action Item:

Update auditor workpapers based upon work performed by the audit team, including sample testing.

Action Item Purpose:

The purpose of this action is to document all information, data, testing results, and audit team conclusions in the workpapers.

The purpose of this action is to review findings and other selected areas from section 02-0501 with the audit team. Compliance Auditor judgments and any deviations from the audit objectives are documented within the workpapers. The Compliance Auditor consults with the ATL on these judgments, samples, audit conclusions, and deviations from planned testing approaches. If necessary, the ATL will include Audit Management to discuss possible judgments and deviations from the audit objectives.

Action Item Steps

1. Documentation includes:
   a. Specific registered entity-supplied files that were reviewed for each Reliability Standard and Requirement
   b. Identification of the section within the document that supports any audit conclusions
   c. Follow-up questions and evidence requests for the registered entity SMEs
   d. Conclusions that have been identified
   e. Conclusions supporting the observations and findings that are made for each Reliability Standard and Requirement
   f. Note and define any tick marks used during testing
2. Document all aspects of testing and methodology that include:
   a. Inquiry
   b. Observation
   c. Physical examination
   d. Documentation review
   e. Reperformance
   f. Confirmation
3. Complete the Auditor Checklist Action Item.

Action Item Highlights

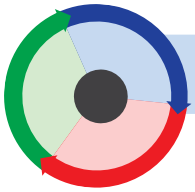
Action Owner: Audit Team Lead
Action Reviewer: Not Required
Final Approver: Not Required
Action Timing: During Audit Testing

Action Item Tips & Techniques

1. Document results of testing in a manner that an experienced auditor can understand.
2. Reasonable assurance may require more than one form of testing to reduce audit risk.
3. Testing documentation/evidence needs to be sufficient and appropriate to support audit conclusions.
4. When documenting, include the document, page, and section for ease of reference.
5. Registered entity work practices or processes/ procedures being performed should be captured and documented.
6. Cross collaboration with other audit teams on-site is important for obtaining complete information.
7. Keeping workpapers by Requirement can help a Compliance Auditor organize his or her activities.
8. Keeping a summary of No Findings in an external document facilitates the completion of audit objectives.

Action Item References

1. GAGAS – Sections 6.73 – 6.77 and 6.79 – 6.85
2. IIA-IPPF – Standards 2310 and 2340



02-0700 | Audit Fieldwork >> Documenting Findings

02-0700

Task Overview:

The purpose of this Task is to assure that audit conclusions are appropriately documented and reviewed by the ATL and the audit team. Documentation must support the finding and be detailed enough to enable an experienced auditor unrelated to the audit to reperform the testing and reach the same conclusion. The ATL needs to be adequately prepared to discuss conclusions that have been reached with the registered entity's PCC.

Action Items

Action Item #	Action Item
02-0701	Document Findings

Task Highlights

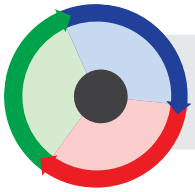
The Task is considered complete when the audit team conclusions are confirmed, documented, and supported with evidence.

Key Documents to Complete:

- Workpapers
- Supporting evidence

Task Timing:

- During the audit



02-0101

Action Item:

Document elements of findings. The following should be considered during documentation of findings:

- **Criteria:** Scoped Reliability Standard and Requirements
- **Condition:** The situation that exists – degree and extent of compliance with the Criteria
- **Cause:** Reason or explanation for the condition
- **Effect or potential effect:** Clear, logical link to establish impact – actual and potential risk to BPS as a result of the Condition
- Populating the Workpapers

Action Item Purpose:

The purpose of this action is to assure that audit documentation has sufficient detail to enable an experienced auditor to understand the audit evidence and the resulting conclusions. Audit findings must include reference to documented evidence.

Action Item Steps

1. Reference all relevant evidence related to the finding in the workpapers.
2. Conclusions should include *(as applicable)*:
   a. Criteria *(Reliability Standard version being tested)*
   b. Condition
3. When a determination of a Potential Noncompliance or Area of Concern is made, the Compliance Auditor must document:
   a. Cause
   b. Effect
   c. Timing
4. Review finding to confirm all relevant evidence is included and that all evidence cited in the finding is documented in the workpapers.
5. Complete the Auditor Checklist Action Item.

Action Item Highlights

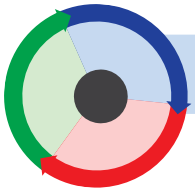
Action Owner: Audit Team Lead
Action Reviewer: Not Required
Final Approver: Audit Team Lead
Action Timing: During Audit Testing

Action Item Tips & Techniques

1. Sufficiency of audit team conclusions consists of professional judgment and appropriate evidence as well as levels of qualitative and quantitative evidence.
2. Remember that positive observations may be noted within the audit report.
3. Write findings with audiences in mind, such as registered entity, Audit Management, and Enforcement staff.
4. OEAs must be considered with regard to conclusions.

Action Item References

1. GAGAS – Sections 6.73-6.77
2. IIA-IPPF – Standard 2330 and 2410; Practice Advisory 2410-1



02-0800 | Audit Fieldwork >> Audit Team Debrief

02-0800

Task Overview:

The purpose of the Task is for the audit team to prepare their work and to perform an internal discussion to prepare for meeting with the registered entity's PCC. The audit team will need to pay special attention to the conclusions reached and supporting evidence. The task includes:

- Quality review of the workpapers
- Discussion of conclusions for audit team consensus
- Discussion of conclusions with registered entity *(allow them to submit additional supporting or mitigating evidence)*
- Permit additional testing to verify the breadth and depth of the audit team conclusions
- Notify the registered entity PCC that the audit team is ready to meet

Action Items

Action Item #	Action Item
02-0801	Discuss conclusions internally with the audit team

Task Highlights

The Task is considered complete when:

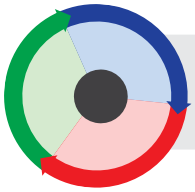
1. Workpapers have been reviewed
2. Conclusions have been discussed internally
3. Conclusions have been discussed with the registered entity
4. Any additional testing has been scheduled

Key Documents to Complete:

- Workpapers
- Talking points or templates

Task Timing:

- During the audit



02-0801 | Audit Fieldwork >> Audit Team Debrief >> Internal Discussion and Evidence Review

02-0801

Action Item:

Discuss conclusions internally with the audit team.

Action Item Purpose:

The purpose of this action is to both prepare the audit team(s) to meet with the registered entity's PCC to deliver a status of the audit activities to date, and to actually meet with the PCC and give the status. The team(s) should assemble the work they have completed and discuss the level of completion and information that must be discussed.

Action Item Steps

1. Meet with the audit team to review work product for the day and discuss:
   a. Status of assigned work
   b. Outstanding data requests or requests for additional information and data
   c. Evidence of audit team conclusions
   d. Verify evidence has been placed in workpapers
2. Document in the workpapers as necessary.
3. The ATL reviews the following at the periodic audit team meeting:
   a. Reliability Standards and Requirements still open
   b. Conclusions
   c. Potential concerns or possible roadblocks that affect the audit objectives
   d. Noteworthy observations
   e. Schedules and remaining activities
4. Discuss impacts to other team(s) on the audit engagement. The ATL communicates the timing and activities that support the completion of audit objectives.
5. Communicate engagement changes to Audit Management.
6. Resolve and document inconsistencies in documentation or testing approaches.
7. Determine if additional testing or audit work is required to meet audit objectives.
8. Review roles and responsibilities of the audit team in preparation for meeting with the registered entity's PCC.
9. Finalize the status for presentation to the registered entity's PCC.
10. Notify the registered entity's PCC that the audit team is ready to meet.
11. Complete the Auditor Checklist Action Item.

Action Item Highlights

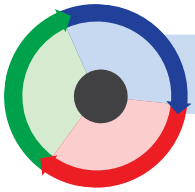
Action Owner: Audit Team Lead
Action Reviewer: Audit Team Lead
Final Approver: Not Required
Action Timing: Daily activity during the audit

Action Item Tips & Techniques

1. Audit team caucuses periodically during the day supports preparation for this activity.
2. Prepare daily activities to support debriefing and status meetings. Build time into the schedule to account for unplanned events.
3. Keep the ATL apprised of impacts to audit objectives.
4. Anticipate impacts to audit timing and testing.
5. Documenting the work when it is performed facilitates preparation for discussion with the audit team.
6. Status checks and communication are critical to the success of an audit engagement.
7. Utilize regional tools for tracking and reviewing audit team conclusions *(e.g., RFC-CMP macro based Microsoft Excel workbook)*.
8. On-site audits should include daily audit team meetings.
9. Off-site audit team meetings may be conducted at different intervals based on audit circumstances.

Action Item References

1. GAGAS – Sections 6.73 -6.77 and 6.79 – 6.85
2. IIA-IPPF – Standard 2400 and Practice Advisory 2410-1



02-0900 | Audit Fieldwork >> Status Briefing

02-0900

Task Overview:

The purpose of this Task is for the ATL and audit team to conduct status briefings with the registered entity's PCC to discuss open items, progress, and conclusions. The timing for briefings depends on on-site and off-site audit timing and the ATL must consider the frequency and timing accordingly.

Action Items

Action Item #	Action Item
02-0901	Conduct status meetings with the registered entity's PCC in order to review open action items, discuss audit team conclusions, and other audit matters

Task Highlights

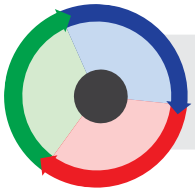
The Task is considered complete after the ATL conducts the status briefing with the registered entity's PCC.

Key Documents to Complete:

- Workpapers
- Briefing documentation

Task Timing:

- During the audit



02-0901 | Audit Fieldwork >> Status Briefing >> Audit Status Meetings

02-0901

Action Item:

Conduct status meetings with the registered entity's PCC in order to review open action items, discuss conclusions, and other audit matters.

Action Item Purpose:

The purpose of this action is for the ATL and audit team to meet with the registered entity's PCC to provide the status of activities associated with completing the audit objectives. The registered entity's PCC should understand work completed, remaining activities, additional evidence requests and testing that is being performed, and should discuss conclusions. The audit team should also be prepared to answer any questions posed by the registered entity's PCC. The action also provides the audit team an opportunity to periodically verify the accuracy of its conclusions before the audit reaches the Reporting Phase.

Action Item Steps

1. During these status meetings, the ATL reviews with the registered entity's PCC:
   a. Conclusions that have been identified to date
   b. Scheduling of additional SME interviews and confirmation of the dates and times of any interviews already scheduled
   c. Additional potential concerns or possible roadblocks
   d. New and pending evidence requests
2. Allow the registered entity's PCC an opportunity to provide feedback on the audit. This provides an opportunity to express any concerns, and gives the ATL an opportunity to address issues in a timely manner.
3. Provide a copy of the daily debrief to the registered entity's PCC and Audit Management.
4. Document daily status meeting and relevant information in the workpapers.
5. Complete the Auditor Checklist Action Item.

Action Item Highlights

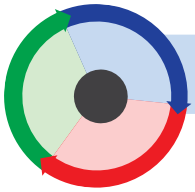
Action Owner: Audit Team Lead
Action Reviewer: Not Required
Final Approver: Not Required
Action Timing: During the audit

Action Item Tips & Techniques

1. Audit team should conduct daily status meetings for on-site audits. This includes communicating the conclusions to the PCC in a timely manner and not at the end of the audit.
2. Off-site status meetings may be conducted at different intervals based on audit circumstances.
3. Continue consistent and clear communication with registered entity's PCC. Status meetings should support and confirm the conversations held periodically during the day.
4. Resolve any communication conflicts and implement process improvements.
5. Confirm turnaround times on evidence requests.
6. Audit team should actively listen to the registered entity's PCC and personnel.
7. Attend NERC-sponsored Crucial Conversations training.

Action Item References

1. GAGAS – Section 6.78
2. IIA-IPPF – Standard 2400 and Practice Advisory 2410-1



02-1000 | Audit Fieldwork >> Audit Team Conclusions

02-1000

Task Overview:

The purpose of the Task is to evaluate the audit team final conclusions, verify facts, compile supporting documentation, and prepare for reviews with the registered entity's PCC and the audit team prior to exit briefings.

An audit team conclusions review consists of:

- Validating the testing to verify it is supported by sufficent and appropriate evidence
- Classifying through audit team consensus
- Ensuring they are thoroughly documented
- Discussing Findings with Management and/or Enforcement, as necessary

Action Items

Action Item #	Action Item
02-1001	Gather the audit team to reconfirm the relevance, validity and supporting documentation of the findings including a thorough description of the audit work performed to derive the findings.

Task Highlights

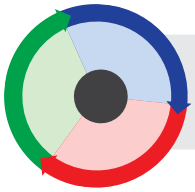
The Task is considered complete when the ATL has reviewed and verified conclusions.

Key Documents to Complete:

- RSAWS

Task Timing:

- During the audit



02-1001 | Audit Fieldwork >> Audit Team Conclusions >> Validating Audit Conclusions

02-1001

Action Item:

Gather the audit team to reconfirm the relevance, validity, and supporting documentation of the final conclusions.

Action Item Purpose:

The purpose of this action is for the audit team to review and confirm the sufficiency and appropriateness of documentation that supports conclusions of the audit. Workpapers must include a thorough description of the work performed, and evidence appropriately referenced and documented.

Determine if the facts and circumstances of the Potential Noncompliance have potential impact on other Reliability Standards and Requirements. The audit team should also consolidate the findings and determine if there is an apparent underlying commonality of cause, as well as risk to the BPS, and/or provide process improvement suggestions.

Action Item Steps

1. ATL to lead team review to verify all conclusions are supported by sufficient and appropriate evidence that is linked to the conclusions in the workpapers:
   - Cite page and paragraph in connection with supporting documentation
   - Document other facts and circumstances that may be applicable
   - Evidence may also consist of unique identifiers *(e.g., access control list, query language used for sampling, files, folders, drawings, etc.)*
2. Evaluate whether a Potential Noncompliance impacts or leads to the potential failure of compliance with another Reliability Standard or Requirement.
3. For each Potential Noncompliance, if possible, prepare an evaluation by reviewing and documenting:
   - Applicable Reliability Standard and Requirement
   - Start date and stop date
   - Actual and potential risk to BPS reliability
   - Controls that are associated with the Potential Noncompliance
   - Any mitigating actions planned or already taken by the registered entity
   - Whether it is an indicator of a problem with their compliance culture and program
4. Determine if the audit scope should be expanded or additional monitoring methods should be scheduled in the future *(e.g., Spot Check, Self-Certification, or other monitoring method)*.
5. Complete the Auditor Checklist Action Item.

Action Item Highlights

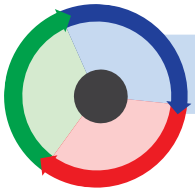
Action Owner: Audit Team Lead
Action Reviewer: Not Required
Final Approver: Not Required
Action Timing: Through the conclusion of the audit

Action Item Tips & Techniques

1. Audit evidence must include how it supports the finding and not just be listed.
2. Workpapers and RSAWs should be appropriately-cross-referenced.
3. The Finding should have documentation that is sufficient and appropriate, stands on its own, and is auditable.
4. Tools used to track and manage evidence outlined in the RSAWs should be used accordingly, by Region.
5. Region specific documents or tools may be used in lieu of the RSAW to record specific evidence references.

Action Item References

1. GAGAS – Sections 6.69 -6.77 and 6.79 – 6.85
2. IIA-IPPF – Standard 2400 and Practice Advisory 2410-1
3. CMEP – Sections 3.1.1 and 3.8



02-1100 | Audit Fieldwork >> Exit Briefing

02-1100

Task Overview:

The Task of conducting the Exit Briefing includes:

- Creating the Exit Briefing
- Reviews by the appropriate individual(s)
- Scheduling of the Exit Briefing
- Establishing the medium of communication *(e.g., webinar)*
- Delivering the Exit Briefing
- Documenting the Exit Briefing in the workpapers

Action Items

Action Item #	Action Item
02-1101	Prepare the Exit Briefing presentation and meet with PCC and registered entity management to discuss results of the audit including Potential Noncompliances, Areas of Concern, and Recommendations

Task Highlights

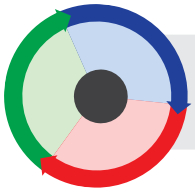
The section is considered complete when the Exit Briefing is presented and delivered to the PCC.

Key Documents to Complete:

- Exit Briefing presentation
- NERC feedback form
- Workpapers

Task Timing:

- The audit end date



02-1101

Action Item:

Prepare and deliver the Exit Briefing presentation.

Action Item Purpose:

The purpose of this action is to:

1. Create the Exit Briefing presentation for delivery to the registered entity. The briefing shall include any findings or results from the audit. The presentation must include the following:
   - Review of the audit scope
   - Descriptions of the Potential Noncompliance, Areas of Concern, Recommendations, and any additional observations
   - An overview of the next steps for the registered entity after the audit
2. Review all exit materials and discussion points before meeting with the PCC. The audit team reviews the contents of the Exit Briefing presentation to verify the completeness and accuracy of the audit results and to verify there are no grammatical or spelling errors.
3. Conduct a meeting with representatives from the registered entity to review the results from the audit and answer any questions. The ATL coordinates with the PCC to determine the time and location. Exit Briefings may occur the last day of fieldwork or on a date agreed upon between the PCC and the ATL.

Action Item Steps

1. Develop the Exit Briefing presentation
2. Develop talking point notes that may not be a part of the presentation documentation.
3. If Regional Entity policy allows the registered entity to maintain evidence documentation on behalf of the Region, the following protocol should be followed:
   a. Place all evidence on one or two copies of recordable media
   b. Perform a strong cryptographic hash of the evidence files
   c. Place the recordable media in a Tyvek envelope (or equivalent)
   d. Retention instruction should be placed inside and marked on the outside of the container
   e. Provide to the PCC for physical custody
   f. Retain a copy of the hash list in the workpapers
   g. Create and maintain a chain of custody
4. Audit team to review all Exit Briefing presentation material.
5. Meet with the PCC to:
   a. Set the date, time and place of the Exit Briefing
   b. Inform the PCC of all Findings before the meeting
   c. Provide the PCC with an update on OEAs' status
   d. Provide the presentation material for the Exit Briefing or determine the method of delivery
6. Conduct the Exit Briefing and answer any questions.
7. Provide the PCC with the NERC feedback form template and requested return date.
8. Review the audit report comment timing and purpose with the PCC.
9. Store the Exit Briefing in the workpapers.
10. Complete the Auditor Checklist Action Item.

Action Item Highlights

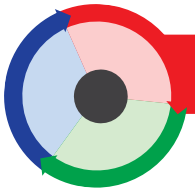
Action Owner: Audit Team Lead
Action Reviewer: Audit Management *(as needed)*
Final Approver: Audit Team Lead
Action Timing: The audit end date

Action Item Tips & Techniques

1. Use the (Regional) Exit Briefing template to develop the presentation.
2. Don't use a prior audit's presentation.
3. Recommendations should include *(if applicable)*:
   a. Specific facts and circumstances
   b. Explanation of risk
   c. Possible solutions
4. Acronyms are to be initially spelled out and properly defined.
5. Allot the appropriate time for the completion and review of the presentation material.
6. Perform grammar and spell check. Read the presentation and do not rely only on electronic verification.
7. Verify that embedded markings from previous presentations are appropriately removed.
8. Verify communications are neutral in tone and speak to the issue.
9. Be mindful of your audience for the Exit Briefing *(executives and others who not have participated in the audit)*.
10. Compliance Auditors are encouraged to seek training on building and delivering presentations.
11. Preview the presentation with the PCC.
12. Make sure equipment is charged and/or has fresh batteries.
13. Be familiar with equipment being used and plan accordingly.
14. Use Exit Briefings as development opportunities for presentation skills.
15. Use a non-confrontational tone during the briefing.
16. Presentations need to be fact based and clearly supported with evidence.
17. Webinars and teleconferencing are acceptable for briefings.
18. Informal meetings are encouraged so that open discussion with the registered entity management can take place.
19. Audit team attendance at the Exit Briefing is recommended.
20. Compliance Auditors should attend presentation training.

Action Item References

1. GAGAS – Sections 6.78 and 7.14 – 7.18
2. IIA-IPPF – Standard 2400
3. CMEP – Section 3.1.1



03-0000 | Audit Reporting

Area Overview:

Audit Reporting consists of all activities following the completion of Audit Fieldwork. Audit Reporting consists of seven (7) Tasks and their associated Action Items. The Audit Reporting Area consists of three primary activities: the drafting and completion of the audit report, management of the workpapers, and performing a self-assessment relative to the completed audit.

Reporting: Audit reports communicate the results of each completed audit. Audit reports are developed to facilitate communication of audit conclusions and results with representatives from the registered entity, Regional management, NERC, and FERC. Reports must be prepared in a clear, specific, and neutral manner and fact based.

Workpapers: Compliance Auditors must document relevant information to support the conclusions and engagement results. Workpapers are audit records that must be maintained in a secure manner for an appropriate retention period.

Lessons Learned: Compliance Auditors continuously improve through constructive self-assessment and reflective analysis. Meeting as a team to discuss and document observations, feedback, and suggestions is a capstone activity of the audit. Lessons learned should be shared across the ERO Enterprise.

Tasks

Task #	Task
03-0100	Workpaper Review
03-0200	Communicating with Enforcement
03-0300	Draft Report Creation
03-0400	Delivery of Draft Report
03-0500	Final Report
03-0600	Workpaper Management
03-0700	Lessons Learned

P-03

Audit Reporting:

Reporting is the final step for completing the audit and is accomplished by communicatiing results, compiling audit records for retention, assessing audit successes, and identifying opportunities for improvement. Reports must focus on providing clear and concise messages with well-supported conclusions. The audit team and the ATL must communicate with Enforcement *(and/or Assessment/Mitigation, Analytics)* staff regarding all Potential Noncompliances and Areas of Concern to assure all facts and circumstances are understood for proper determination.

Auditors should be familiar with:

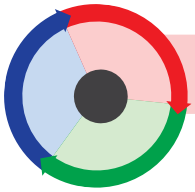
- ✓ Professional writing
- ✓ Time management
- ✓ NERC audit reporting
- ✓ Presentation skills

Key Documents to Complete:

- Quality Assessment Template
- Public and non-public Report
- Auditor Checklist

Guiding Documents:

- GAGAS – Chapter 7
- IA-IPPF – Standard 2400
- CMEP – Section 3.1.6



03-0100 | Audit Reporting >> Workpaper Review

03-0100

Task Overview:

Workpapers are the documentation of record that substantiate the planning and execution of the audit and support conclusions drawn as a result of the audit work completed. The purpose of this Task is to review and verify that workpapers are complete and accurate and they convey the audit history. In addition to Quality Assessments, Audit Management on a sample basis, will routinely review and verify workpaper documentation for timeliness, completeness, accuracy, and consistency.

Action Items

Action Item #	Action Item
03-0101	Review workpapers for completeness, accuracy, and quality

Task Highlights

The Task is completed when the workpaper review is performed and the Audit Checklist is complete.

Audit documentation must be consistent in both quality and detail as well as between Compliance Auditors and across various engagements.

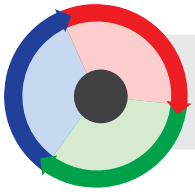
Audit Management review of workpapers is critical for verifying that Compliance Auditors execute with the same degree of precision and rigor.

Key Documents to Complete:

- Auditor Checklist
- Quality Assessment Template *(as required)*

Task Timing:

- ATL Review
- Management Review - as scheduled



03-0101 | Audit Reporting >> Workpaper Review >> Audit Team Lead Workpaper Review

03-0101

Action Item:

Review workpapers for completeness, accuracy, and quality.

Action Item Purpose:

The purpose of this action is to finalize workpapers to support the delivery of Potential Noncompliances to Enforcement, draft the audit report, and finalize assembly of all pre-audit, planning and fieldwork documentation. The ATL performs a review of all workpapers for completeness, accuracy, and quality.

Action Item Steps

1. Move all documentation into an appropriately secured audit document repository.
2. Verify RSAWs and documentation exists to support audit objectives *(not a complete list)*:
   a. Planning documents
   b. Interview sheets
   c. Field notes
   d. Physical examination notes
   e. Registered entity-maintained documentation
   f. Culture of compliance workpapers
   g. Regional Entity-specific documentation and work files *(refer to Regional process)*
3. Verify documentation and supporting evidence can be found within the workpapers and workpapers can be tied to and support the audit conclusions.
4. Resolve workpaper discrepancies identified through the review.
5. Delete or destroy duplicate documents and data in accordance with record management controls.
6. Denote record retention timing for deletion and destruction of workpapers.
7. Complete the Auditor Checklist Action Item.

Action Item Highlights

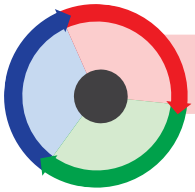
Action Owner: Audit Team Lead
Action Reviewer: Audit Team Lead
Final Approver: Not Required
Action Timing:

Action Item Tips & Techniques

1. Directory finding tools are beneficial for performing an inventory and tracking documents *(e.g., Directory List Print Pro, FSUM and FSUM Front End are suggested tools)*.
2. Scanning hard copies facilitates electronic assembly of workpapers.
3. Folder structure and file naming conventions are strongly encouraged.
4. Storing evidence by Reliability Standard and Requirement facilitates accessing data.

Action Item References

1. GAGAS – Section 6.83
2. CMEP – Section 3.1.6



03-0200 | Audit Reporting >> Communicating with Enforcement and Risk Assessment

03-0200

Task Overview:

The purpose of this Task is to provide Enforcement *(and/or Assessment/Mitigation/Analytics)* staff with necessary documentation and support to seamlessly transition identified Potential Noncompliance. The communication assists in verifying the understanding of the Findings, mitigating actions or plans, and the extent of condition of the issue(s). The Task is complete when the Potential Noncompliances are submitted to and reviewed with Enforcement.

Action Items

Action Item #	Action Item
03-0201	Meet with Enforcement *(Risk Assessment/Mitigation/Analytics Staff)* post-audit to discuss the findings and convey pertinent information.
03-0202	Provide Risk Assessment Department any lessons learned /entity information obtained during the audit that could result in an update to the entity's IRA

Task Highlights

Possible Violations need to be communicated to Enforcement *(and/or Assessment/ Mitigation/Analytics)* staff.

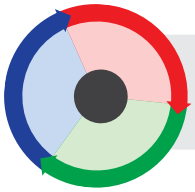
The Team notifies Enforcement *(and/or Assessment/ Mitigation/ Analytics)* staff of the existence, technical nature, and risk to the Bulk Power System.

Key Documents to Complete:

- Potential noncompliance documentation

Task Timing:

- Timing of coordination with Enforcement regarding Possible Violations is specific to each Regional Entity's handoff processes
- Possible Violations must be report within five days of the final determination



03-0201 | Audit Reporting >> Communicating with Enforcement and Risk Assessment >> Enforcement Discussions

03-0201

Action Item:*

Meet with Enforcement *(Risk Assessment/Mitigation/Analytics Staff)* post-audit to discuss the findings and convey pertinent information.

Action Item Purpose:

The purpose of the action is to submit Potential Noncompliance(s) and supporting documentation to Enforcement *(and/or Assessment/Mitigation/Analytics)* staff in conformance with the ROP processes and to meet with Enforcement as necessary. Meetings may occur with Enforcement *(and/or Assessment/Mitigation/Analytics)* staff at any time to review the Potential Noncompliance(s), supporting documentation and facts and circumstances, and to answer any questions.

** This Action Item does not apply if there are no Potential Noncompliances resulting from the audit.*

Action Item Steps

1. All Potential Noncompliance(s) must be submitted to Enforcement within five business days of the Exit Briefing.
2. Conduct a meeting with Enforcement *(and/or Assessment/Mitigation/Analytics)* staff to review Potential Noncompliances and any additional relevant information that substantiates the basis for the Potential Noncompliance(s) and explains the risk to the BPS. Support should consist of:
   a. Reliability Standard and Requirement
   b. Affected dates
   c. Supporting material
   d. Mitigation plans and completed actions *(as applicable)*
   e. Statement of risk to the BPS
   f. FFT recommendation *(as applicable)*
   g. Extent of Condition *(as applicable)*
   h. Compliance Exception (CE)/Find, Fix, Track & Report (FFT) recommendation
3. Document the meeting and update the workpapers.
4. Complete the Auditor Checklist Action Item.

Action Item Highlights

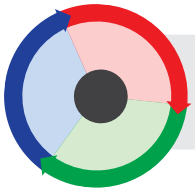
Action Owner: Audit Team Lead
Action Reviewer: Audit Management
Final Approver: Audit Management
Action Timing: Five days from determination of a Potential Noncompliances all other as needed.

Action Item Tips & Techniques

1. Submit Potential Noncompliances through the appropriate portal *(e.g., webCDMS or CITS)*.
2. Update Enforcement (*and/or Assessment/Mitigation/Analytics)* staff throughout the engagement to keep them apprised of Findings during the audit.

Action Item References

1. GAGAS – Sections 6.79 - 6.85, 7.24 – 7.26
2. CMEP – Section 3.1.1, 3.8
3. IA-IPPF – Standard 2400 and Practice Advisory 2410-1



03-0202 | Audit Reporting >> Communicating with Enforcement and Risk Assessment >> Feedback to IRA Development Team

03-0202

Action Item:

Provide Risk Assessment Department any lessons learned/entity information obtained during the audit that could result in an update to the entity's IRA.

Action Item Purpose:

The purpose of the action is to provide timely feedback to the IRA development team of anything that is pertinent learned during the audit that potentially could result in a change to the IRA.

Action Item Steps

1. Communicate with Risk Assessment staff to review lessons learned, results of the audit, results of internal controls evaluations *(if applicable)*, issues related to Reliability Standards *(clarity and/or inconsistency)*, and any other relevant information that should be factored into the IRA.
2. Complete the Auditor Checklist Action Item." in the Action Item Box.

Action Item Highlights

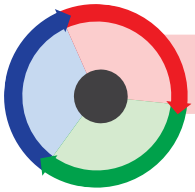
Action Owner: Audit Team
Action Reviewer:
Final Approver:
Action Timing:

Action Item Tips & Techniques

ATL debriefing to Risk Assessment staff to be performed according to Region specific RA procedures as appropriate.

Action Item References

1. GAGAS – Section 3.95



03-0300 | Audit Reporting >> Draft Report Creation and Handoff to Management

03-0300

Task Overview:

The purpose of the Task is for the ATL to create the draft audit report. The draft audit report contains valid conclusions that are substantiated by the workpapers. Audit Management is responsible for reviewing and approving the draft report prior to sending it to the PCC and NERC.

Action Items

Action Item #	Action Item
03-0301	Compile ERO standard draft report describing the results of the testing along with any Potential Noncompliances, Areas of Concern, and Recommendations
03-0302	Perform independent management review of the draft report, including verifying report content supported by sufficient and appropriate evidence

Task Highlights

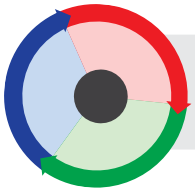
The draft audit report is created to summarize the conclusions of the audit engagement for review by the PCC.

Key Documents to Complete:

- Draft audit report

Task Timing:

- Varies based on Regional processes



03-0301 | Audit Reporting >> Draft Report Creation and Handoff to Management >> Preparing the Draft Report

03-0301

Action Item:

Compile ERO standard draft report describing the results of the testing along with any Potential Noncompliances, Areas of Concern, and Recommendations.

Action Item Purpose:

The purpose of this action is to prepare the draft report using the ERO non-public Audit Report Template. The ATL is responsible for completion of the draft non-public report. The audit team reviews the draft report to confirm that both the objectives of the audit and the audit results are accurately documented. Any discrepancies that are identified are forwarded to the ATL for correction.

Action Item Steps

1. Draft the report using the ERO non-public Audit Report Template.
2. Refer to RSAWs and other workpapers to support the report content.
3. The ATL notifies the audit team the draft report is ready for review and comment.
4. The ATL sets the deadline for review and comment completion.
5. Audit team reviews the draft report for the following:
   - Audit objectives have been addressed in the draft report
   - Findings are written clearly and objectively and are properly supported
   - Proofing errors *(e.g., spelling, punctuation, grammar, cut-and-paste errors)*
   - Review header and footer links
   - Review the start/stop dates with implementation guidance
6. Update the draft report for all comments and update the table of contents.
7. Notify Audit Management that the document is ready for review.
8. Complete the Auditor Checklist Action Item.

Action Item Highlights

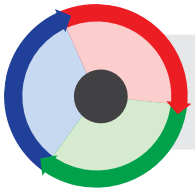
Action Owner: Audit Team Lead/Compliance Program Coordinator
Action Reviewer: Audit Team Lead
Final Approver: Not Required
Action Timing:

Action Item Tips & Techniques

1. Source documents and resources:
   a. Audit Notification Packet
   b. Registration database
   c. Pre-audit survey
   d. Other pre-audit and planning phase documentation
2. Write the draft report in plain language.
3. Determine if draft report needs to be translated.
4. Mail Merge assists with populating the document.
5. Check footers, headers, and red text color.

Action Item References

1. GAGAS – Sections 7.03 – 7.31
2. IIA-IPPF – Standard 2400
3. CMEP – Section 3.1.6



03-0302 | Audit Reporting >> Draft Report Creation and Handoff to Management >> Management Review

03-0302

Action Item:*

Audit team Lead hands off draft report and workpapers to Audit Management for review.

Action Item Purpose:

The purpose of the action is to provide Audit Management with a draft version of the non-public report for review and comment in preparation for submission to the registered entity. It is also for Audit Management or a designee to perform a secondary review on a sample basis to verify the completeness of documentation and accuracy of workpapers and associated determinations.

** This Action Item does not apply if there are no Potential Noncompliances resulting from the audit.*

Action Item Steps

1. The ATL notifies Audit Management the draft non-public report and workpapers are ready for review and comment.
2. The ATL finalizes the draft non-public report based on Audit Management comments, obtains final approval, and prepares for submission to the PCC and NERC.
3. Complete the Auditor Checklist Action Item.

Action Item Highlights

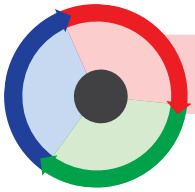
Action Owner: Audit Team Lead/Audit Management
Action Reviewer: Audit Management
Final Approver: Regional Mgmt
Action Timing:

Action Item Tips & Techniques

1. Draft audit report meets the requirements of the CMEP and NERC guidance.
2. Review the start/stop dates with implementation guidance.
3. The ATL performs a final review using **page preview**, verifies font type and size, and other formatting changes that may have occurred.
4. Share observations with the entire audit team on learning opportunities and best practices.

Action Item References

1. GAGAS – Sections 7.03 – 7.31
2. IIA-IPPF – Standard 2400
3. CMEP – Section 3.1.6



03-0400 | Audit Reporting >> Delivery of Draft Report

03-0400

Task Overview:

The purpose of the Task is to send the approved draft audit report to the PCC and NERC in a timely manner. The PCC is afforded the opportunity to provide comments on the report, which may or may not be incorporated into the final report.

Action Items

Action Item #	Action Item
03-0401	Provide the draft non-public report to PCC for comment and to NERC. Update the draft report with any comments received from the entity

Task Highlights

The Task is considered complete when the approved draft audit report is sent to the PCC for comment.

Key Documents to Complete:

- Finalized draft report

Task Timing:

- Varies based on Regional processes

03-0401

03-0401 | Audit Reporting >> Delivery of Draft Report >> Provide Draft Report to Registered Entity

Action Item:

Provide the draft non-public report to PCC and to NERC for comment. Update the draft report with any comments received from the entity.

Action Item Purpose:

The purpose of the action is to finalize and provide the draft non-public report to the PCC. The PCC provides comments on the draft report prior to finalization.

Non-public Reports contain information that is confidential; they are handled according to the Regional Entity's polices regarding confidential documents.

Action Item Steps

1. The ATL reviews all Audit Management comments.
2. Finalize document for delivery:
   a. Accept changes
   b. Save the document according to NERC naming conventions
3. Secure the draft report for delivery to the PCC according to appropriate Regional protocol.
4. The ATL/CPC transmits the draft report to the PCC with instructions on when and how responses are to be provided and provide the draft report to NERC per the current protocol.
5. The ATL confirms receipt of the draft non-public report by the PCC.
6. The ATL receives any feedback from the PCC for consideration.
7. Update the non-public report with comments submitted by the PCC, as appropriate, in preparation for finalizing the report.
8. Complete the Auditor Checklist Action Item.

Action Item Highlights

Action Owner: Audit Team Lead/Compliance Program Coordinator
Action Reviewer: Audit Team Lead
Final Approver: Not Required
Action Timing:

Action Item Tips & Techniques

1. If Microsoft Word is used to submit the report, a review should include removal of hidden text, comments, red-lines, etc.
2. Do not send draft reports via non-secure means.
3. Update any information that is not material to audit determinations *(e.g., misspelled names and titles)*.

Action Item References

1. GAGAS – Sections 7.32 – 7.38 and 7.44
2. IIA-IPPF – Standard 2420
3. CMEP – Section 3.1.6

03-0500 | Audit Reporting >> Final Report

Task Overview:

The purpose of the Task is to perform final reviews and edits to the audit report, and deliver the final report to the PCC and NERC.

Action Items

Action Item #	Action Item
03-0501	Create final version of non-public and public *(as applicable)* reports
03-0502	Submit final non-public and public *(as applicable)* report to the PCC. 1. Public reports are not provided for CIP audits 2. Public reports are only provided to the PCC immediately if there are no Potential Noncompliances 3. If there are Potential Noncompliances or OEAs, the public report is provided to the PCC after all Enforcement actions and mitigations are complete
03-0503	Submit final non-public and public *(as applicable)* report to NERC. 1. Public reports are not provided for CIP audits 2. Public reports are only provided to the PCC immediately if there are no Potential Noncompliances 3. If there are Potential Noncompliances, the public report is provided to the PCC after all Enforcement actions and mitigations are complete

Task Highlights

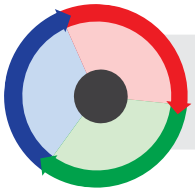
The Task is considered complete when the final report(s) is provided to the PCC and NERC.

Key Documents to Complete:

- Final audit report(s)

Task Timing:

- Non-public reports –
- Public reports *(as available)*:
  a. Filing with the non-public report when there are no Potential Noncompliances or Open Enforcement Actions, or
  b. Completion of Enforcement and mitigating activities



03-0501 | Audit Reporting >> Final Report >> Create Final Report

03-0501

Action Item:

Create final version of non-public and public *(as applicable)* reports.*

** CIP reports are non-public only.*

Action Item Purpose:

The purpose of the action is to finalize the non-public and public reports *(as applicable)* based on any additional information and final discussions with the PCC and/or Audit Management.

Action Item Steps

1. ATL to create the **public report** by editing the **non-public report**, in accordance with NERC Reporting Guidelines.
2. Check with Audit Management to determine if a final review is needed based on any changes.
3. Save the audit report in the workpapers.
4. Complete the Auditor Checklist Action Item.

Action Item Highlights

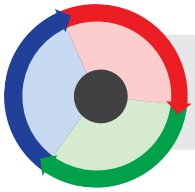
Action Owner: Audit Team Lead/Compliance Program Coordinator
Action Reviewer: Audit Management *(as needed)*
Final Approver: Not Required
Action Timing:

Action Item Tips & Techniques

1. Discuss PCC requested changes with Audit Management.
2. Do not use the PCC submitted version of the draft report as the source document for the final report.
3. The final report should be formatted in Adobe Acrobat for submission to the PCC and NERC.
4. Reconfirm the Adobe Acrobat file has been edited to remove hidden information and other metadata.

Action Item References

1. GAGAS – Sections 7.39 – 7.43
2. IIA-IPPF – Standard 2420
3. CMEP – Section 3.1.6
4. NERC Reporting Guidelines



03-0502 | Audit Reporting >> Final Report >> Submit Non-Public Report

03-0502

Action Item:

Submit final non-public report to the PCC and NERC.

Action Item Purpose:

The purpose of the action is to deliver the final report to the PCC and NERC.

Action Item Steps

1. Deliver the non-public report to the PCC and NERC in an approved secure manner.
2. Confirm delivery of the report(s) to the PCC.
3. Email NERC to notify them of delivery of the report and request a confirmation.
4. File confirmations of receipt in the workpapers.
5. Complete the Auditor Checklist Action Item.

Action Item Highlights

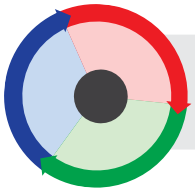
Action Owner: Audit Team Lead/Compliance Program Coordinator
Action Reviewer: Audit Management
Final Approver: Audit Management
Action Timing:

Action Item Tips & Techniques

1. Send the report with a delivery confirmation and read receipt.
2. Follow-up with a phone call to the PCC if a confirmation receipt is not received.

Action Item References

1. GAGAS – Sections 7.39 – 7.44
2. CMEP – Section 3.1.6



03-0503 | Audit Reporting >> Final Report >> Submit Public Report

03-0503

Action Item:

Submit final public report (as applicable) to the PCC and NERC.

1. *Public reports are not provided for CIP audits.*
2. *Public reports are only provided to the PCC and NERC immediately if there are no Potential Noncompliances.*
3. *If there are Potential Noncompliances, the public report is provided to the PCC and NERC after all Enforcement actions and mitigations are complete*.

Action Item Purpose:

The purpose of this action is to submit the final public reports to the PCC and NERC after Enforcement processes are complete if Potential Noncompliances were found during the audit.

Action Item Steps

1. If there were no Potential Noncompliances identified, the public audit report can be sent to the PCC and NERC at the same time as the non-public report.
2. If the public report is not submitted with the non-public report, the Regional Entity must track the completion of Enforcement and mitigation activities. The public report is then submitted to the PCC and NERC after the completion of Enforcement and mitigation activities.
3. Confirm delivery of the report to the PCC.
4. Email NERC to notify them of delivery of the report and request a confirmation.
5. File confirmations of receipt in the workpapers.
6. Complete the Auditor Checklist Action Item.

Action Item Highlights

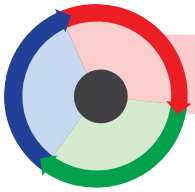
Action Owner: Audit Team Lead/Compliance Program Coordinator
Action Reviewer: Audit Management
Final Approver: Audit Management
Action Timing:

Action Item Tips & Techniques

1. The ATLs and Compliance Program Coordinator should request access to the NERC website before reports being due.
2. The Regional Entity is encouraged to have more than one authorized user to submit audit reports to the secure folder.

Action Item References

1. GAGAS – Sections 7.39 – 7.44
2. CMEP – Section 3.1.6



03-0600 | Audit Reporting >> Workpaper Management

03-0600

Task Overview:

The purpose of the Task is to review workpapers and complete close out activities related to the management of audit documentation. The process includes placing required documentation into a secure format, establishing the retention period, and ensuring the audit team has appropriately disposed of non-essential, redundant, and sensitive audit data. The Task consists of three (3) actions that must be completed.

Action Items

Action Item #	Action Item
03-0601	Perform an inventory check of all relevant workpapers and supporting documentation
03-0602	Archive the workpapers
03-0603	Obtain confirmation from all team members that audit related data was removed from hard drives, shared drives, thumb drives, or any other media, including the destruction of hard copies of documents and auditor notes

Task Highlights

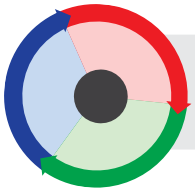
The Task is complete when documentation has been placed in a secure format, retention schedules are confirmed, and the ATL has confirmed the audit team has appropriately disposed of audit material.

Key Documents to Complete:

- None

Task Timing:

- Varies based on Regional processes



03-0601 | Audit Reporting >> Workpaper Management >> Workpaper Completeness and Approval

03-0601

Action Item:

Perform an inventory check of all relevant workpapers and supporting documentation.

Action Item Purpose:

The ATL and the audit team are responsible for performing a quality review of the workpapers to confirm that files applicable to the audit appear in the appropriate workpaper locations. These reviews are also performed to verify that all audit conclusions are supported by sufficient workpaper documentation. If any content appears to be missing or inaccurate, the audit team works together until there is a resolution. The purpose of the action is also to provide Audit Management with an opportunity to review the workpapers as necessary and sign-off on their completion. This action may also serve as a second level confirmation that supporting workpapers exist and are in the appropriate locations within the files.

Action Item Steps

1. A final workpaper review should consist of:
   a. Review workpapers for key documents cited in the audit report
   b. Compare the RSAWs to documents noted in the audit report
   c. Verify that the workpapers contain final versions of the Inherent Risk Assessment, scoping, communications with the PCC, sampling requests, surveys, etc.
2. Review electronic folders or document management system for content.
3. Verify that relevant emails have been captured and consolidated.
4. Correct, add, or delete any documentation identified as a result of the review.
5. Custodial agreements for eveidence retained by the entity are documented in the workpapers.
6. Ask the audit team to delete and destroy sensitive documentation and unnecessary documentation as needed.
7. The ATL confirms the workpapers are completed and ready for Audit Management review.
8. The ATL makes any modifications to the workpapers resulting from the Audit Management review.
9. Sign off workpapers as final.
10. Complete the Auditor Checklist Action Item.

Action Item Highlights

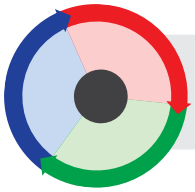
Action Owner: Audit Team Lead
Action Reviewer: Audit Management
Final Approver: Audit Management
Action Timing:

Action Item Tips & Techniques

1. Convert all hard copy documents to electronic form for storage.
2. Compliance Auditors verify that workpapers meet Regional Entity procedural filing requirements
3. Audit Management provides best practices to improve audit techniques and approaches.

Action Item References

1. GAGAS – Sections 7.39 – 7.44
2. CMEP – Section 3.1.6



03-0602 | Audit Reporting >> Workpaper Management >> Archive the Workpapers

03-0602

Action Item:

Archive the workpapers.

Action Item Purpose:

The purpose of the action is to lock all documentation and archive the approved workpapers.

Action Item Steps

1. Utilize Regional Entity archive methods to preserve the integrity of workpapers, evidence, and reports.
2. Complete the Auditor Checklist Action Item.

Action Item Highlights

Action Owner: Audit Team Lead/Compliance Program Coordinator
Action Reviewer: Not Required
Final Approver: Audit Team Lead
Action Timing:

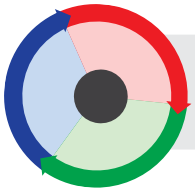
Action Item Tips & Techniques

1. Processes related to archiving documents should consider:
   - Retention periods
   - Folder and file security
   - Secure passwords and encryption tools for future access to documentation
   - Migration of files
   - Physical retention
2. The registered entity must also make documentation available for Enforcement and third parties in connection with reviews being conducted by NERC, FERC or other authorized organizations.
3. Archiving of RE documents be performed according to Region specific procedures as appropriate.

NERC and FERC should contact the Regional Entity before contacting the registered entity.

Action Item References

1. GAGAS – Sections 3.91 – 3.95



03-0603 | Audit Reporting >> Workpaper Management >> Post Audit Data Destruction

03-0603

Action Item:

Obtain confirmation from all team members that audit related data was removed from hard drives, shared drives, thumb drives, or any other media, including the destruction of hard copies of documents and auditor notes.

Action Item Purpose:

The purpose of the action is to reconfirm with the audit team that all documentation, evidence, and data has been appropriately removed, deleted, and destroyed.

Action Item Steps

1. Notify audit team that the workpapers are archived and that any remaining files, documents, and evidence can be safely destroyed. Remind Compliance Auditors to check all recordable media devices such as hard drives and thumb drives, as well as hard copy files.
2. Request Compliance Auditors confirm the above activity is complete.
3. Complete the Auditor Checklist Action Item.

Action Item Highlights

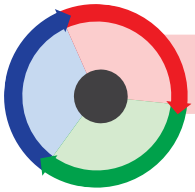
Action Owner: Audit Team Lead
Action Reviewer: Not Required
Final Approver: Not Required
Action Timing:

Action Item Tips & Techniques

1. Evidence in electronic form should be encrypted *(according to Regional Entity policy).*
2. Do not take physical evidence to another registered entity location *(this includes audit notes, copies of the audit report, etc.).*
3. Confirmations from the Compliance Auditors should be placed with workpapers.

Action Item References

1. GAGAS – Sections 3.91 – 3.95
2. CMEP – Section 9



03-0700 | Audit Reporting >> Lessons Learned

03-0700

Task Overview:

The purpose of the Task is to provide an opportunity for the audit team to meet either with or outside of Audit Management to review feedback provided by the registered entity and discuss the audit team's personal observations. The audit team discussion includes:

- Reviewing comments from the registered entity feedback form
- Identifying and sharing best practices
- Documenting lessons learned
- Disseminating information within and across regions

Action Items

Action Item #	Action Item
03-0701	Discuss leading practices and opportunities for improving throughout all stages of the audit cycle

Task Highlights

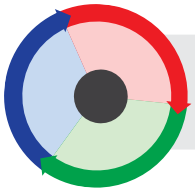
The Task is complete when the audit team has met, reviewed feedback, and documented lessons learned for future use.

Key Documents to Complete:

- Lessons learned documentation

Task Timing:

- Varies based on Regional processes



03-0701 | Audit Reporting >> Lesson Learned >> Post-Audit Discussions

03-0701

Action Item:

Discuss leading practices and opportunities for improving throughout all stages of the audit cycle.

Action Item Purpose:

The purpose of the action is to meet with the audit team and conduct a debrief meeting to review the registered entity feedback form as well as discuss leading practices, lessons learned, audit experience, and industry knowledge to improve the overall audit practice. While this is a continuous learning process throughout the course of the audit, final discussion and documentation should be completed.

Action Item Steps

1. The ATL schedules the post-audit meeting.
2. The ATL reviews feedback from the registered entity.
3. If NERC or FERC were observers on the audit, request their feedback for discussion.
4. Conduct the post-audit discussion. Identify recommendations and observations that require action plans or process improvement.
5. Document the discussion, provide a summary to Audit Management and place the notes in the workpapers.
6. Identify areas that may be included in Regional Entity and NERC auditor workshops for training and lessons learned.
7. Complete the Auditor Checklist Action Item.

Action Item Highlights

Action Owner: Audit Team Lead/Management
Action Reviewer: Not Required
Final Approver: Not Required
Action Timing:

Action Item Tips & Techniques

1. Identify opportunities to share lessons learned with other Regional Entities through:
   a. Communication of best practices
   b. Regional Entity training panel discussions
2. Share relevant information with other departments within the Regional Entity.
3. Collect leading practices, tools, templates, and processes and share with the ERO Staff Training Group on a periodic basis.
4. Share lessons learned regarding the registered entity and audit techniques between CIP and Operation and Planning.

Action Item References

1. GAGAS – Sections 3.91 – 3.95
2. IIA-IPPF – Standard 1300

Auditor Checklist

P-01

01-0000 | Audit Planning

P-02

02-0000 | Audit Fieldwork

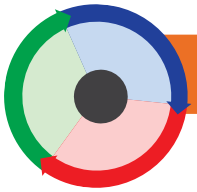
P-03

03-0000 | Audit Reporting

Auditor Checklist

Area	Task #	Task	Action Item #	Action Item
Audit Planning 01-0000	01-0100	Audit Scoping	01-0101	ATL to obtain the IRA and COP, and develop the Audit scope.
	01-0200	Assemble and Brief the Audit Team	01-0201	Assign and document roles and responsibilities.
			01-0202	Establish internal project milestones, goals, and expectations.
			01-0203	Provide and review the audit scope and supporting materials, including prior compliance monitoring history, lessons learned, and Inherent Risk Assessment with the audit team.
	01-0300	Confirm Independence	01-0301	Confirm independence and address conflicts of interest for each Compliance Auditor, consultant, and third-party team member.
	01-0400	Prepare Audit Notification Packet	01-0401	**Prepare a preliminary Audit Notification Packet/request list to be sent out to the registered entity, including the following:** • Requests for supporting documentation for the purposes of testing the Reliability Standards • Nondisclosure or Confidentiality Agreements for audit team members • Pre-Audit and Compliance Surveys to be completed by the registered entity
			01-0402	Perform review of the Audit Notification Packet *(person other than the preparer)*.
	01-0500	Send Audit Notification Packet	01-0501	Communicate in writing with the registered entity being audited to cover objectives, audit scope, expectations, logistics, and timing of the audit.
			01-0502	Coordinate a pre-audit meeting with key personnel within the registered entity to discuss the audit, expectations, and any questions related to the information included in the initial Audit Notification Packet.
	01-0600	Sample and Test Agenda	01-0601	Utilize NERC approved ERO Enterprise Sampling Guide to develop samples to test the in-scope requirements, and submit the samples to the entity.

Note: This is the current Auditor Checklist as of September 2017.



Area	Task #	Task	Action Item #	Action Item
Audit Fieldwork 02-0000	02-0100	Preliminary Documentation Review	02-0101	Review the completeness, accuracy, and validity of the supporting documentation requested. Draft follow up inquiries and procedures, identify audit team conclusions, and document gaps. Determine whether additional documentation is required to satisfy the audit objectives.
	02-0200	Additional Documentation Request	02-0201	Evaluate whether the lack of supporting documentation is due to deficiencies or other program weaknesses, and whether the lack of documentation could be the basis for findings.
			02-0202	Send subsequent sample and data requests when required.
	02-0300	Final Planning Meeting	02-0301	Schedule and conduct a final planning meeting to discuss expectations, milestones, agenda, status communication protocol, and additional preparatory activities.
	02-0400	Conduct Opening Presentation	02-0401	Conduct the opening presentation meeting to reconfirm expectations, milestones, and status communication protocol.
	02-0500	SME Interviews	02-0501	**Conduct interviews with the registered entity. The following should be considered during the discussions:** • Understand the policies, procedures, and processes by which the registered entity complies with the relevant Reliability Standards • Understand how often the procedures/processes are performed *(i.e., frequency)* • Confirm who owns and performs each policy/procedure/process • Assess the competency *(e.g., training, certifications, background)* of the SME or compliance contact responsible for the policy/procedure/process • Understand interview issue/failure escalation process • Document conversations in workpapers
			02-0502	Obtain an understanding of internal controls related to the audit scope.
	02-0600	Documenting Results	02-0601	Update auditor workpapers based upon work performed by the audit team, including sample testing.

Note: This is the current Auditor Checklist as of September 2017.

Area	Task #	Task	Action Item #	Action Item
Audit Fieldwork 02-0000 (Continued)	02-0700	Document Findings	02-0701	**Document elements of findings. The following should be considered during documentation of findings:** • Criteria: Scoped Reliability Standard and Requirements • Condition: The situation that exists – degree and extent of compliance with the Criteria • Cause: Reason or explanation for the condition • Effect or potential effect: Clear, logical link to establish impact – actual and potential risk to BPS as a result of the Condition • Populating the workpapers
	02-0800	Audit Team Debrief	02-0801	Discuss conclusions internally with the audit team.
	02-0900	Status Briefings	02-0901	Conduct status meetings with the registered entity's PCC in order to review open action items, discuss audit team conclusions, and other audit matters.
	02-1000	Audit Team Conclusions	02-1001	Gather the audit team to reconfirm the relevance, validity and supporting documentation of the final conclusions.
	02-1100	Exit Briefing	02-1101	Prepare and deliver the Exit Briefing presentation.

Note: This is the current Auditor Checklist as of September 2017.

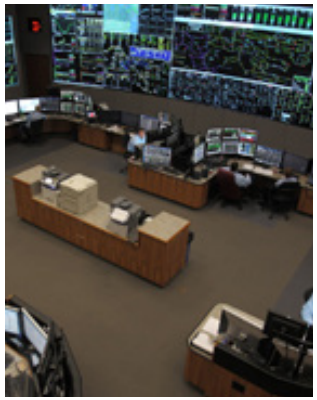
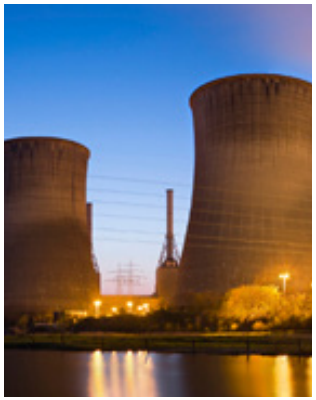
Auditor Checklist

Area	Task #	Task	Action Item #	Action Item
Audit Reporting 03-0000	03-0100	Workpaper Review	03-0101	Review workpapers for completeness, accuracy, and quality.
	03-0200	Communicating with Enforcement and Risk Assessment	03-0201	Meet with Enforcement *(Risk Assessment/Mitigation/Analytics Staff)* post-audit to discuss the findings and convey pertinent information.
			03-0202	Provide Risk Assessment Department any lessons learned/entity information obtained during the audit that could result in an update to the entity's IRA.
	03-0300	Draft Report Creation and Handoff to Management	03-0301	Compile ERO standard draft report describing the results of the testing along with any Potential Noncompliances, Areas of Concern, and Recommendations.
			03-0302	Audit Team Lead hands off draft report and workpapers to Audit management for review.
	03-0400	Delivery of Draft Report	03-0401	Provide the draft non-public report to PCC for comment and to NERC. Update the draft report with any comments received from the entity.
	03-0500	Final Report	03-0501	Create final version of non-public and public *(as applicable)* reports.
			03-0502	Submit final non-public report to the PCC and NERC.
			03-0503	Submit final public *(as applicable)* report to the PCC and NERC. 1. Public reports are not provided for CIP audits. 2. Public reports are only provided to the PCC immediately if there are no Potential Noncompliances. 3. If there are Potential Noncompliances or OEAs, the public report is provided to the PCC after all Enforcement actions and mitigations are complete.
	03-0600	Workpaper Management	03-0601	Perform an inventory check of all relevant workpapers and supporting documentation.
			03-0602	Archive the workpapers.
			03-0603	Obtain confirmation from all team members that audit related data was removed from hard drives, shared drives, thumb drives, or any other media, including the destruction of hard copies of documents and auditor notes.
	03-0700	Lessons Learned	03-0701	Discuss leading practices and opportunities for improving throughout all stages of the audit cycle.

Note: This is the current Auditor Checklist as of September 2017.

ERO ENTERPRISE

Sampling Guide

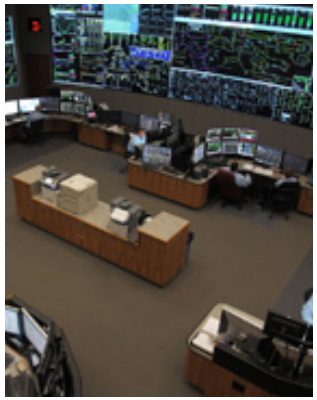
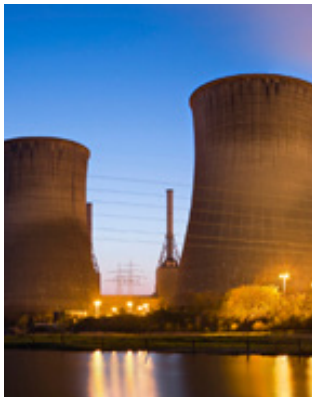



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

VERSION 4 | 2018

ERO ENTERPRISE

Sampling Guide (Cont.)...

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

VERSION 4 | 2018

SAMPLING GUIDE | TABLE OF CONTENTS

INTRODUCTION | CHAPTER 1

This document provides guidance when using sampling as a tool for compliance monitoring of Registered Entities (Entities). Regional Entity (Region) staff is responsible for identifying the sampling approach appropriate for the compliance monitoring method. This document is divided into the following sections: Overview, Sampling Approaches, Sampling Table A, and Sampling Glossary, with Appendices A, B, and C. These sections comprise the ERO Sampling Guide.

Background

The Compliance Monitoring and Oversight Process Working Group (CMPWG) developed a sampling methodology included in the ERO Sampling Guide. During the creation of the ERO Handbook in 2013, a need to update the ERO Sampling Guide was identified. Similarly, the Key Reliability Standards Spot-Check (KRSSC); PRC-005-1 Key Reliability Standard Spot-Check, September 14, 2011 noted a need to update the ERO Sampling Guide. With the approval of the ERO Compliance and Enforcement Group (ECEMG) and NERC, the ECEMG assigned the Manual Task Force (MTF) to create an updated Sampling Guide that can be used by all Compliance Enforcement Authority (CEA). The MTF worked with the Compliance Monitoring Functional Group (CMFG) to create a Sampling Guide that updates the current document and incorporates the new Risk-based Compliance Monitoring and Enforcement Program (CMEP) principles. The Sampling Guide is the culmination of work and input from all eight Regions and various working groups.

Sampling Guide

Chapter 2 - Overview provides information about general sampling concepts and techniques. It also discusses documentation of the sampling process and the workpapers associated with the sampling process.

Chapter 3 - Sampling Approaches offers two categories of sampling approaches: Statistical and Non-statistical. This is to generate consistent and confident sampling.

Chapter 4 - Sample Table A and Appendix A-Sample Table A further establish a minimum set of guidelines for use with various compliance monitoring activities. These sampling approaches are also recognized by Generally Accepted Government Auditing Standards (GAGAS) and the Institute of Internal Auditors (IIA).

Additionally, **Chapter 5** - Sampling Glossary and the illustrative examples in Appendix B offer further guidance on different approaches to performing both Statistical and Non-statistical Sampling. Refer to the glossary in **Chapter 5** for additional information on any of the technical or capitalized terms referenced in this document. Finally, Appendix C provides the Lead Sheet Template.

OVERVIEW | CHAPTER 2

This chapter provides information about the use of general sampling approaches to sample evidence when performing various compliance monitoring activities. Sampling is essential for auditing and compliance monitoring because it is not always possible or practical to test 100% of either the equipment elements or documentation artifacts.

In the audit context, there are generally two primary approaches to sampling: Statistical and Non-statistical. Auditors may use a combination of the Statistical and Non-statistical approaches as well as other approaches to sampling. Regardless of the sampling approach, the CEA should determine the approach based on testing objectives. If the objective is to ensure a higher level of confidence concerning compliance that can be extrapolated to the whole population, for instance, the CEA should use Statistical Sampling. The CEA should appropriately document the chosen sampling approach, testing objective(s), supporting details, confidence level, and associated testing conclusions in the workpapers. Where Statistical Sampling is not practical, the CEA should establish criteria basis and context and document the justification of the value(s) and testing results of the Non-statistical sample selected.

Compliance Management or the Team Lead may determine, through the use of an Inherent Risk Assessment (IRA) and/or Internal Controls Evaluation (ICE) review, that the number of samples can be reduced for the engagement. If the number of items sampled is below those established in the Sampling Handbook, the CEA shall document in the workpapers the rationale for reducing the size of the sample population.

Overview of Sampling Process

Preparation Inputs (PI)

Document Review Type, Entity, Preparer, Reviewer, Dates, W/P & RSAW cross reference info

Identify & Describe Source Population(s) & Type(s):

- Primary Population - (Statistical)
- Dependent/Secondary - (Statistical/Judgmental)
- Independent Population
- Specific Populations - (not Primary, Dependent or Independent Populations)

Preparation Inputs (PI)

- Obtain & Review the Source Population Record Layout
- Identify Data Points, Field Values or Elements for Selection & Testing
- Determine Alignment of Records History & Sampling Time Period
- Validate Source Population for Data Integrity & Completeness

Process Activities (PA)

- Document the Sampling Testing Objective(s):
- If Applicable, Select the Testing Objective from the Requirements Menu:

*PER-005	*CIP-002
*PRC-005	*CIP-004
*FAC-003	*CIP-005
*FAC-008	*CIP-007
*COM-002	*CIP-009
	*Etc.

Process Activities (PA)

- Identify & Describe Impactful Risk and Internal Control Considerations:
- Select & Document Sampling Approach & Rationale:

*Statistical (Random)	*Judgmental
*Statistical Stratified (Random)	*Other
*Non-Statistical	

Process Activities (PA)

Determine the Initial Sampling & Size:

- Document Relevant Time Periods Considered
- Select Sample Size Based on Table A or Sampling Tool *(e.g., RAT-STATS)*
- Determine Sample Using an Automated Sampling Tool
- Document Statistical Sampling Metrics where applicable: Confidence Level, Margin of Error, Random Seed Number, Precision, Rate of Occurrence, etc.

Test Results Output (TRO)

- Assess & Document Test Sampling Results in Line with Stated Testing Objectives
- Document if Sampling Approach Requires Expansion or Modification
- Document Basis for Expanded Sampling
- Document Basis for Deviations in Sampling or Planned Testing Procedures

OVERVIEW | CHAPTER 2

Risk-Based Approach

The risk-based approach includes the Inherent Risk Assessments (IRA) performed by the Regions. This may also include an Internal Controls Evaluation (ICE) by the Regions. These activities (IRA, ICE, self-audit, self-spot check, data sampling, procedure updates, etc.) help the CEA determine the compliance monitoring process used. This enables the CEA to determine the risk-based scope to use in assessing whether the Entity meets the NERC and Regional Standards. The various risk, control, and compliance activities will support the idea of scoping or reducing the sampling to verify compliance. This will be determined by the CEA teams that review the activities performed by the Entity and Entity's risk to the Bulk Power System (BPS).

Additionally, Entity -performed sampling *(as determined during an Entity's self-evaluation)* may affect the sampling approach chosen. Before relying on the work of others, verify the sampling is unbiased, independent, complete, statistically-based, and well-documented. This can also be used if the CEA team reviews the Entity's samples and determines to expand the sample set. The CEA would then increase the sample set to the number in this document or greater depending on the testing, scope, and objectives of the tests. The determined sampling approach and rationale shall be documented in the workpapers.

Multi-Regional Registered Entities (MRRE)

Multi-Regional Registered Entities (MRRE) are Entities registered for functions in multiple Regions. Under the MRRE there will be at least one lead Region with the other Regions possibly participating or relying on the lead Region to perform the compliance monitoring for all the Regions involved. The MRRE process will require considerable coordination among the Regions as the IRA for the Entity may vary in each of the respective Regions depending on the identified risks, assets, locations, etc. All of the Regions involved should agree on the final scope of a compliance monitoring activity so that risks identified in each of the Regions can be addressed during the activity.

Some sampling considerations that need to be decided to address Entity risk and BPS reliability are as follows:

- Should the population include assets, devices, etc. from all Regions?
- Should the sample include more of the assets, devices, etc. from areas that pose the most risk? Note that the population should be chosen relative to the risk determined by each Region.
- Should the final sample list include *(as an example)* 33 samples from each Region or 33 samples across the Entity's entire population?
- Lead Region shall work with affected Regions to determine the sampling approach

The idea is to develop a sufficient sample of items to reach a level of confidence that the sample is accurate, complete, and meets the testing objectives. The sampling should not be an onerous task to show compliance. The determined sampling approach and the rationale shall be documented in the workpapers.

Requirements with Short Retention Periods

Some NERC Reliability Standards have requirements stating information shall be kept for a short retention period. These requirements usually have a 90-day retention period for very large quantities of data. For example IRO-001-1.1, CIP-005-3a, CIP-006-3c, and CIP-007-3a, among others, all have requirements with the 90-day retention period for data. For compliance monitoring, these requirements require sampling to collect and review a representative group of the total population, thus impacting data for the audit period identified in the monitoring process notification letter. Therefore these factors need to be considered when selecting samples for requirements with short retention periods.

Sampling from Multiple Versions of a Standard

There are several currently enforceable Reliability Standards that have implementation plans which overlap the different versions of the same standard. PRC-005 versions 1 and 2 are examples on the Operations and Planning list. CIP has several Reliability Standards where an Entity may cover two or more versions of the same standard. The CEA needs to ensure the testing meets the objectives for the versions in effect. The CIP version 3 to 5 transition introduces even more overlap.

These version changes can cause confusion for the CEA, as well as the Entity. When compliance monitoring needs to sample for a Requirement over a period of time where there is more than one version of the Reliability Standard in effect, the chosen sampling approach needs to reflect the objectives of the compliance monitoring activity.

Questions to consider include the following: “Are we more concerned with how the Entity supports the newer Requirement” or “How well did the Entity manage the prior versions of the standard?” These questions can lead to a different sampling approach.

The sample set should not be overly burdensome, and the CEA should have some rationale behind the number of samples requested for each version of the standard. However, CEA may choose not review data from the period when the older version of the standard was active because associated Requirements are covered in the newer version of the Requirement, or vice versa. Alternatively, the testing may include multiple samples from the different versions of the Standard. No matter the sampling approach chosen, the approach needs to tie to the overarching monitoring objective, and the CEA must document the approach in the workpapers.

Sampling from Multiple Versions of a Standard (Cont.)...

Data Retention

If current Reliability Standards are silent as to a data retention period, sampling of data should focus on the most recent two years, unless the data sample would be statistically too small or irregularities are identified in the initial samples. This would not apply to the following:

- Voice and audio recordings should focus on a 90-day rolling retention period.
- Standards requiring a current program or procedure should focus on the currently effective version, with a revision history specifying changes and dates of review.
- Standards requiring testing intervals *(e.g., PRC-005)*, should focus on the most recent full testing records with evidence of previous testing intervals.
- For standards supported by evidence records that extend beyond the audit period, the most recent record should be tested. For example, PER-005-1 Requirement R2 requires validation of the most recent competence records for a system operator, even if the date of the record is outside the audit period.

The data retention section is based on the NERC Final Data Retention Whitepaper, September 12, 2014, posted on the NERC Website.

Documentation in Workpapers

In general, compliance monitoring workpapers should reflect the statistical or non-statistical testing approach used and sampling results achieved when performing specific compliance monitoring testing. The workpapers should capture the testing approach in sufficient detail so a reviewer can understand the testing approach used.

The testing or sampling process typically starts with profiling and documenting the type of sampling source population(s) and defining the compliance or other testing objective(s). CEA also determine the sampling approach *(i.e., statistical or non-statistical)*, statistical metrics setting *(e.g., Confidence Level, Margin of Error, Precision, etc.)*, sizing of the sample(s), or choosing an alternative sampling method when applicable.

The CEA should document its results of the test sample output and its determinations. The CEA must also substantiate its rationale for any deviations from either the Sampling Handbook guidelines or planned testing procedures within the workpapers. Additionally, the CEA should clearly annotate and provide references for the sample testing outputs or results to aid in analysis and compliance monitoring. Sample output records and results should also be retained and secured in a fashion similar to other workpapers, including supporting evidence and fieldwork evaluations.

The overall workpaper documentation should be of sufficient quality and substance to support management's or an independent third party's review.

The Sampling Guide also references a Sampling Lead Sheet, included as Appendix C, that can be used by the CEA when performing various compliance tests where sampling is used. The Sampling Lead Sheet can be used to capture and catalog the various sampling activities encountered in any given compliance monitoring or other sampling testing. Refer to the Sampling Lead Sheet to reference and catalog sequencing of the various sampling activities.

SAMPLING APPROACHES | CHAPTER 3

Considerations for Professional Judgment When Sampling

Professional judgment has to be exercised throughout the compliance monitoring processes. There are times where the sample population may require a mix of sampling techniques to create the final sample population. This may occur due to the type of data available, timing, logistics, etc., that affect the compliance monitoring process. The team should be able to justify why a particular method is used during an engagement. The reasoning and variations shall be documented in the workpapers. The Sampling Handbook does not dictate how a population is sampled but provides guidance on common practices used by the ERO to perform sampling. The CEA always has the flexibility to sample a population as it sees fit to meet the objectives.

Statistical Sampling

Statistical Sampling is employed when testing the entire population is impractical but one wants to extrapolate the results of the test over the entire population. Statistical Sampling provides assurance that the attributes of the selected sample represent the entire population. Using RAT-STATS or other Statistical Sampling tools together with the Sampling Handbook further supports this approach to compliance monitoring testing. The CEA may also use information gathered during the engagement to increase or lessen the sample size for Statistical Sampling. This information may come from the IRA, ICE, or other documentation already reviewed to justify modifying the sample size. When the sample size is reduced, the confidence level is also reduced for that population. If the sample size is increased, the confidence level is also increased for that population.

The Sampling Handbook and its predecessor, the ERO Enterprise Sampling Guide, are based on the use of a 95% confidence level, which is represented in Sample Table A. Should a different confidence level be employed, the CEA will have to use a Statistical tool *(such as RAT-STATS)* to determine the sample size. The ideology behind the 95% confidence level is to sample a representative portion of the total population with a low margin of error (MOE).

It is recommended that CEA opt for the 95% confidence level as opposed to selecting a higher confidence level *(e.g., 98% or 99%)*. This is because as the confidence level increases, the number of standard errors also increases along with the MOE. If you wish to be more than 95% confident about your results, you will need to add and subtract more than two standard errors. For example, 99% confidence requires the addition and subtraction of 2.58 standard errors *(i.e., critical value or z*-value)* to derive the MOE. Therefore, the higher the confidence level, the larger the z*-value, the larger the MOE, and the wider the confidence interval. Hence, there is an added price for seeking the additional confidence. It should be noted the wider confidence interval and increased margin of error can both be offset and reduced, respectively, by increasing the sample size. Refer to the glossary in Chapter 5 for additional information on any of the technical terms referenced in this section.

The CEA needs to document the use of Sample Table A or the use of a different confidence level or sample size and note the other materials used to justify this decision in the workpapers.

Statistical Sampling (Cont.)...

Considerations for Statistical Sampling (Single Random)

It should be noted that in a simple random sample of a given size, all subsets of the population frame are given an equal probability. Any given element from a set of selected elements (pairs, triples, and so on) has the same chance of selection as any other. This minimizes bias and simplifies analysis of results. Statistical Sampling (Simple Random) may be vulnerable to sampling error when the randomness of the selection sample does not reflect the population composition. In this case, the CEA may wish to consider using the stratified or systematic sampling techniques, which use information about the population to choose a more representative sample.

Considerations for Statistical Sampling (Stratified)

Where source populations can be differentiated by unique categories, the population frame can be organized by these categories into homogenous "strata." Each stratum can be sampled as an independent sub-population from which individual elements can also be randomly selected. This approach typically allows for greater specificity of the sampled results. Additionally, becuase each stratum is treated as an independent population, different sampling approaches can be applied to different strata.

As an example, if there are ten substations in the total population, with three at 345kV and seven at 230kV, then this would be a population with two different strata. An example of homogenous strata would be the five different Protection System Device types. Sampling all the relays and the integrated components associated with the relay *(CT/PT, DC circuitry, communications, and DC sources)* would create a homogenous set of data.

This type of sampling can be accomplished in two ways: first you could sample the five separate component populations, or second you can sample the relays and request all associated components for each relay selected.

Considerations for Statistical Sampling (Systematic)

Systematic sampling relies on arranging the study population according to an ordering scheme and then selecting elements at regular intervals through the ordered list. Systematic sampling requires a random start and then proceeds with the selection of every kth element [(k=population size/sample size] from then onwards. The starting point is chosen randomly from within the 1st to the kth element in the list. For example, sampling every 5th item is also known as an every 5th sample or as a "sampling skip of 5." This approach can be especially efficient for sampling from databases. With a randomized starting point, this approach represents a type of probability sampling. The practitioner should also be aware that the Statistical Sampling (Systematic) approach can be vulnerable to periodicities in the list. If list periodicity is present and the period is a multiple or factor of the systematic interval used, then the sample is likely to be unrepresentative of the overall population.

Non-statistical Sampling

There may be cases where Statistical Sampling is inappropriate for obtaining the desired or stated testing objective. For example, consideration of Events Analysis or an IRA further requires the evaluation of a particular subset of the population. In this case, a Non-statistical approach *(Judgmental, etc.)* is used to augment the initial Statistical sample.

Considerations for Judgmental Sampling

Some situations and populations do not fit the statistical models. This demonstrates the need for the CEA to add items to the selected sample list for compliance monitoring activities. Therefore, the population of samples may need to be selected using a Judgmental Sampling process. The Judgmental Sampling process is a useful alternative to Statistical Sampling. This may be due to items being at more risk to the BPS or there is a history of issues with the items selected. The workpapers shall document the reasoning for the selected items, the actual items selected, and the determinations.

Considerations for Attribute-based Sampling

Attribute-based sampling is an alternative approach centered on the concept of control frequency. As an example, this methodology rationalizes that if an attribute executes on a daily basis, then it occurs about 30 times a month. As a result, the CEA selects a sample of 30. If the attribute is an automated one, such as a password configuration, then a sample of one may be obtained. Additionally, if the population is under 10, the CEA would test the entire population. If the audit population is under 30, the CEA would test one for each 24-hour day. Additionally, it should be noted that attributes that are regularly exercised *(e.g., daily)* result in a high confidence rating.

SAMPLE TABLE A

The Sample Table in Appendix A is designed to provide the CEA more guidance after the sampling approach (Statistical and Non-statistical) is determined. The table includes three sections, each with a range of numerical spreads that support a confidence factor of 95% with a +/- 10% MOE. The sample selection value is based upon the minimum value of the population size.

When the population sample to be reviewed consists of documentation records, a Statistical approach using RAT-STATS or other Statistical tools is expected. The Statistical Sampling process is divided into two applications:

- The first application is where the population needs to be reduced in steps consisting of a Primary and Dependent sampling group to select the final sample set. A Statistical sample is selected from the Primary population to create a Dependent population for sampling. From the Dependent population, the final sample set is selected. The selection of Dependent samples may be repeated to refine the population until a final sample set is selected.

- The second application is where the population is independent and can be statistically sampled from the original population. The population size determines the number of samples selected.

- Non-statistical Sampling is addressed in Chapter 3. Non-statistical Sampling is performed when the population to be reviewed is physical, restricted by travel and time constraints, or other instances where a Judgmental sampling process would better address the sampling of the population and meet the objectives.

From the selected sample set, the CEA can then use Statistical Sampling to select the final items to review. As an example, Non-statistical Sampling is used to select substations to visit. Then from the list of substations, a Statistical Sampling method is used to select the items reviewed at the selected substations.

Use of the Sampling Table

Use the first column to identify the description of the population to be sampled. There are three types of populations listed in the table:

a) Statistical Primary and Dependent Populations: used when a large population (substations, ESPs) includes even larger subpopulations (relays, CCAs)

b) Statistical Independent Populations: used when elements are not interdependent with other elements that need to be sampled

c) Non-statistical

Statistical Primary and Dependent Populations

For large populations, identify the Primary population size listed in the first column *(example: substations, etc.*). Once the population is identified, use the second column to determine the sample size to sample from the Primary population. Next use the Primary samples to request the list of items that are relevant to the Primary samples. From the materials received, the Dependent Population has been identified. From the Dependent population, use the first column to select the size of the population and the second column to determine the number of samples to request. This creates a list of sample items identified that will be included in the final data request for that requirement.

a) First: Identify primary population *(substations, etc.)*

   i. If the total number of the primary population of substations owned by the Entity is 1-8, sample the entire population.

   ii. If the total number of the primary population of substations owned by the Entity is greater than or equal to 9, sample 8 of the substations.

b) Second: Identify the total number of secondary-dependent population elements (relays) from the primary population *(substations, etc.)*

   i. If the total number of the dependent population of relays owned by the Entity is 1-9, sample all elements.

   ii. If the total number of the dependent population of relays owned by the Entity is 10-19, sample 9 elements.

Use of the Sampling Table (Cont.)...

Statistical Independent Populations

Identify the Primary population size listed in the first column. Once the population is identified, use the second column to determine the sample size to sample from the population. This creates a list of sample items identified that will be included in the final data request for that requirement.

Non-statistical Populations

Identify the Primary population size that meets the documented criteria for the compliance monitoring *(example, substations within a 60-mile radius)*. Once the population is identified, use the second column to determine the sample size to sample from the Primary population. Note there may be reasons not to sample four items. The CEA will document the criteria and reasoning for its selection of samples. Once the Primary population has been identified, the team will request the list of items that are relevant to the Primary samples. It is preferred that Statistical Sampling is used at this point to refine the final sample list. But there are times where Judgmental sampling would better meet the objectives. The CEA will document the process used and the outcome of the sampling review.

Examples of the sampling process are provided in Appendix B, Sampling Process Flows.

SAMPLING GLOSSARY | CHAPTER 5

The terms included in this section define different methods and concepts associated with the Sampling Handbook:

- **Attribute:** A quality, property, or characteristic.
- **Compliance Monitoring and Enforcement Program (CMEP):** The program used by the North American Electric Reliability Corporation ("NERC") and the Regional Entities to monitor, assess, and enforce compliance with Reliability Standards within the United States.
- **Compliance Enforcement Authority (CEA):** NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.
- **Compliance Monitoring and Oversight Process Working Group (CMPWG):** A retired ERO working group with auditing representatives from all eight Regional Entities and NERC. The group worked to build consistency among the eight Regions. The group was migrated to the CMFG.
- **Compliance Monitoring Functional Group (CMFG):** ERO working group with representatives from all eight Regional Entities and NERC. The group works to build consistency with the compliance monitoring activities for the ERO. The group reports to the ECEMG.
- **Compliance Monitoring Sampling:** The selection and evaluation of a sample of items from a population of relevant information. The CEA expects the sample to be representative of the population and thus likely to provide a reasonable basis for conclusions about the population. In this context, representative means the sample will result in conclusions that, subject to the limitations of sampling risk, are similar to those that would be drawn if the same procedures were applied to the entire population.
- **Confidence Interval:** The single number sample statistic describing a sample (e.g., sample median) plus or minus a margin of error (MOE). The lower end of the interval is the sample statistic minus the margin of error, and the upper end is the sample statistic plus the margin of error.
- **Confidence Level:** A number that marks a level of confidence for which a sample provides a reasonable level of assurance the information reviewed is correct and accurate. The confidence level also represents the confidence interval expressed as a percentage or how confident you are the results will capture the true population parameter depending on the luck of the draw with your sample. The current ERO default is 95%. For more information, see the RAT-STATS user guide.
- **Dependent Sampling:** A sample is chosen from reducing a primary sample population so that a new subset population is created and the dependent samples are selected from it. Example: primary population is "cars", the subset is chosen as "blue cars." Once the list of blue cars is identified, then a final sample set of blue cars can be chosen from the list. This process can be repeated several times to reduce the original population down to a manageable and representative population.
- **Desired Precision Range (Precision):** The range of error, such as plus or minus (+/-) five (5) percent for a 10% precision band. As the range of allowable errors narrows, the required sample size increases. For RAT-STATS, this is the desired width of the confidence interval, with a range of 1-99%. The current ERO default is 10%. For more information, see the RAT-STATS user guide.

SAMPLING GLOSSARY | CHAPTER 5

- **Entity:** When singularly used and capitalized in this document, refers to a Registered Entity as defined in the NERC Rules of Procedure (ROP).

- **ERO Compliance and Enforcement Management Group (ECEMG):** ERO Regional Entity management representing all eight Regions and NERC. The group is comprised of the NERC and Regional compliance operations and enforcement management formed to achieve coordination and collaboration across the ERO Enterprise in the implementation of the CMEP to improve transparency, consistency, efficiency, cost effectiveness, quality, and timeliness of results of compliance monitoring activities.

- **Generally Accepted Government Auditing Standards (GAGAS):** Also referred to as the Yellow Book. This is the professional standards and guidance framework for conducting high quality audits with competence, integrity, objectivity, and independence. This is one of the reference documents used in ERO Compliance Monitoring.

- **Institute of Internal Auditors (IIA):** Is the authoritative guidance as the standard-setting body for the internal audit profession globally. The International Professional Practices Framework (IPPF) is one of the reference documents used in ERO Compliance Monitoring.

- **Independent Sampling:** A sample is chosen from a population that does not need to be sorted or reduced to select a representative sample set.

- **Inherent Risk Assessment (IRA):** IRA of Registered Entities is to identify areas of focus and the level of effort needed to monitor compliance with enforceable NERC Reliability Standards (Reliability Standards). The IRA is a review of potential risks posed by an individual registered entity to the reliability of the Bulk Power System (BPS). An assessment of BPS reliability impact due to inherent risk requires identification and aggregation of individual risk factors related to each registered entity, and the consideration of the significance of BPS reliability impact for identified risks. An IRA considers risk factors such as assets, systems, geography, interconnectivity, prior compliance history, and overall unique entity composition when determining the compliance oversight plan for a Registered Entity.

- **Judgmental Sampling (Non-statistical):** When an auditor selects sample items based on some type of methodology in an attempt to select items that exhibit some type feature. This method purposefully biases the sample, and, thus, the results of the testing cannot be extrapolated to the larger population.

- **Manual Task Force (MTF):** ERO working group tasked with managing the ERO Enterprise Compliance Monitoring and Enforcement Manual. The group consists of four Regional Entity members and a NERC representative. They report to the ECEMG.

- **Margin of Error (MOE):** The number added to a statistic (estimate) of how much the sample results could change if you took another sample. The MOE also equates to the number of standard errors you need to get the confidence level you want. For example, 1.645 standard errors (i.e., critical value) correspond to a 90% confidence level, 1.96 to 95%, 2.33 to 98% and 2.58 standard errors to 99% confidence levels, respectively. Note: Examples based on typical Z-distribution for the critical value (z*-value) and common confidence levels.

- **Multi-Regional Registered Entities (MRRE):** Are registered entities registered for functions in multiple Regions. Under the MRRE there will be one or more lead Regions with the other affected Regions participating or relying on the lead Region to perform the compliance monitoring.

SAMPLING GLOSSARY | CHAPTER 5

- **Non-statistical Sampling:** A sampling approach that does not include both the random selection of the sample items and the use of an appropriate statistical technique to evaluate sample results, including the measurement of sampling risk.

- **Parameter:** A single number that describes a population, such as the median of the population.

- **Population:** The entire set of data from which a sample is selected and about which the compliance monitor wishes to draw conclusions.

- **Random Sampling (Statistical):** See Statistical Sampling.

- **RAT-STATS:** A statistical audit tool used by the U.S. Department of Health and Human Services' Office of Audit Services and developed by the Regional Advanced Techniques Staff (RATS) in San Francisco. The statistical software tool assists the user in selecting random samples. The goal behind RAT-STATS was to develop valuable analytical tools that could be easily used by auditors.

- **Rate of Occurrence:** The expected rate of occurrence for the characteristic within a population. For RAT-STATS, the rate of occurrence is 0.5-98%. The current ERO default is 0.5%. For more information, see the RAT-STATS user guide.

- **Regional Entities (Regions):** The eight regions that make up the North American Electrical Grid. Southwest Power Pool (SPP RE), SERC Reliability Corporation (SERC), Texas Reliability Entity (TRE), Florida Reliability Coordinating Council (FRCC), Midwest Reliability Organization (MRO), Northeast Power Coordinating Council (NPCC), Western Electricity Coordinating Council (WECC), and Reliability First (RF).

- **Seed:** A random number selected by a user of RATS-STATS software to produce a sequence of sample results. Confidential selection of a different seed number prohibits Entities from identifying what items might be selected from a sample population.

- **Sampling:** The act, process, or technique of selecting a suitable sample; specifically, the act, process, or technique of selecting a representative part of a population for the purpose of determining parameters or characteristics of the whole population.

- **Sampling Errors & Biases:** Induced by the sample design. Selection Bias – condition where true selection probabilities differ from those assumed in calculating the results.

- **Random Sampling Error:** Random variation in the results due to elements in the sample being selected at random.

- **Sampling Risk:** The risk the analyst reaches an incorrect conclusion because the sample is not representative of the population or from the correct time period. To correct, adjust the audit procedure *(i.e., selection method/test objective/audit sample size)*.

- **Standard Deviation:** Measures variability (or spread) among the numbers in a data set or distance from the average or mean. It also describes where most of the data should fall (assuming a bell-shaped normal distribution); approximately 95% of the data will lie within two standard deviations of the mean.

SAMPLING GLOSSARY

- **Standard Error:** Measures variability in sample results in terms of a number of standard errors. Similar to standard deviation of a data set - but applies to sample "means" or sample "percentages" that you could have gotten if different samples were taken.

- **Statistic:** A single number that describes a sample, such as the median of the sample. The statistic is typically expressed as a range of possible values for the population parameter. The number that is added to and subtracted from the statistic is called the margin error (MOE) and is denoted by a (+/-).

- **Statistical Sampling:** An approach to sampling that has the following characteristics: a) Random selection of the sample items; and b) The use of an appropriate statistical approach to evaluate sample results, including measurement of the sampling risk.

- **Test/Testing:** The process or approach for evaluating evidence from a registered entity.

SAMPLE TABLE A | APPENDIX A

Sample Table A	
Population Description	**Sample Selection**
Statistical Sampling	
Primary Population (Examples: Substations, Generating Stations, ESPs, PSPs, CCAs)	**Using Statistical Sampling**
1-8	Entire population
9 +	8 Samples
Dependent Population of Elements: (Examples: Relays, CCAs, Routers, Firewalls & Other)	**Using Statistical Sampling**
1-9	All Elements
10-19	9 Samples
20-40	16 Samples
41-100	23 Samples
101-1000	29 Samples
1001 +	33 Samples
Independent Population of Elements: (Examples: Transmission Segments, Blackstart units, Outages, Mis-operations, Daily Operations reports, Line Ratings, others)	**Using Statistical or Judgmental Sampling**
1-9	All Elements
10-19	9 Samples
20-40	16 Samples
41-100	23 Samples
101-1000	29 Samples
1001 +	33 Samples
Non-Statistical Sampling	
Physical Visits : Due to geographic limitations and/or time constraints, the team may choose to sample less than 4 physical sites. (Examples: Control Centers, Substations, Generating Stations)	**Non-Statistical**
1-4	Entire population
5+	4 Samples

The confidence factor is 95% +/- 10% error. Confidence factor is based upon the minimum value of the population span, i.e. for a population range of 10-19; the 95%+/-10% reflects the confidence factor for a population.

SAMPLING PROCESS FLOWS | APPENDIX B

Contents

CIP Standards:

- CIP-007-3
- Additional future examples are being developed

Operations and Planning Standards:

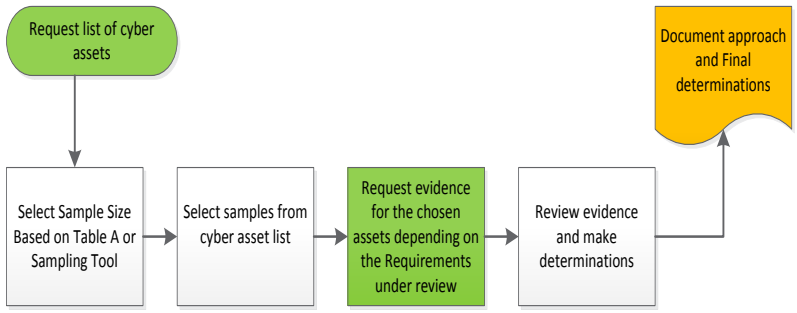
- FAC-008-3
- Additional future examples are being developed

Full sampling examples are posted on the NERC website @ http://www.nerc.com/pa/comp/Documents/Sampling_Handbook_Final_05292015.pdf

CIP-007-3

This may be used for several Requirements.

Flow Chart:



Process:

Request the cyber assets inventory list from the Entity.

Determine the size of the sample set from the Entity approved cyber assets inventory listing by referencing Table A. Then perform the sampling process using a random number generator such as RAT-STATS.

The resulting sample set of cyber asset inventory is then used as the basis for evidence requests relating to the various requirements of **CIP-007-3**. Typical examples of **CIP-007-3** Entity data requests may include:

- **R1.3** - Testing records and results for each selected cyber asset;
- **R2** - Documentation records of enabled ports and services for each cyber asset;
- **R3** - Patch management records for each cyber asset or a complete inventory listing with sampled cyber assets (highlighted);
- **R4** - Evidence that supports up-to-date anti-virus and anti-malware signatures or an approved TFE request for each selected cyber asset;
- **R5.1.2** - Logs of user account access for each cyber asset;
- **R5.2.3** - Provide audit trail records of shared/generic account usage for the cyber asset sample set during the audit period (MM/DD/YY);
- **R5.3** - Provide screenshots or other supporting evidence demonstrating enforcement of password complexity technical requirements, or else provide approved TFE request evidence;
- **R6.4** - Provide security event logs from the audit period (MM/DD/YY) for each cyber asset;
- **R6.5** - Provide supporting evidence that the system event logs generated during the audit period (MM/DD/YY) were reviewed for each cyber asset.

SAMPLING PROCESS FLOWS | APPENDIX B

Comments:

A preliminary meeting between the Compliance Monitoring staff and Entity is often required to gain an understanding of the size and complexity of the Entity organization including telecommunications networking, ESP's, PSP'S, access points, and the number and type of cyber assets. These factors are ultimately considered in determining an effective and suitable approach to sampling. Additionally, as a contingency, RAT-STATS can generate a random number of spares that can be used. Selecting spares provides for additional sample set cyber assets to be tested in place of the initially selected assets where actual results/supporting evidence may not be applicable or available to the initial asset selection.

Availability, format, and size of the data to be sampled during the audit period *(or agreed upon alternative time period)* should be vetted with the Entity. Also, considerations for preserving historical records should be discussed where applicable. Additionally, issues of privacy, confidentiality, or CEII handling should be reconciled with the Entity to ensure the availability of information and records for testing/sampling.

Applicability (Other Standards):

Both the process and sample set can also be utilized in supporting the **CIP-009-3** and **CIP-005-3** standards and requirements. The **CIP-009-3** and **CIP-005-3** compliance monitoring staff may also wish to alter the **CIP-007-3** derived sample set based on professional judgment and the specific needs of their respective requirements. In the case of **CIP-009-3**, consideration should also be given to including and addressing the various cyber asset device types *(e.g., routers, switches, workstations, firewalls, PLC's, etc.)*.

Questions for Data Request:

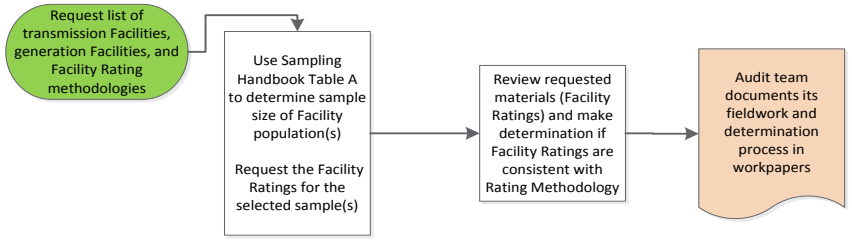
None at this time.

SAMPLING PROCESS FLOWS | APPENDIX B

FAC-008-3

Requirement 6.

Flow Chart:



Process:

Determine Population Size:

Request, if not already available, a list of BPS transmission Facilities and generation Facilities along with the Facility Ratings methodology for each from the Entity. From the total population of BPS transmission Facilities and/or generation Facilities, determine the total population(s) of elements to be sampled.

Determine Sample Size:

This can be accomplished using the Sampling Handbook Table A or RAT-STATS *(or other sampling software)* to define the sample population size(s). Then select the samples using RAT-STATs *(or equivalent tool)* and request the rating data for those samples.

Testing Results:

Review requested materials (Facility Ratings) and make determination if Facility Ratings are consistent with the Ratings Methodology.

Documentation:

Use the Lead Sheet for guidance for various sampling checkpoints; document the sampling approach and audit team determination(s) in audit workpapers.

Comments:

This process applies to Generation Owners (GO) and Transmission Owners (TO). Requirement R6 states the Facility Rating of the generation and transmission Facilities are to be consistent with the Entity's Facility Ratings methodology. Additionally, Regions can further strengthen their evaluations by also performing physical inspections of the Entity Facilities to verify the list of BPS transmission Facilities (generation and transmission) and equipment list (population validation).

Applicability (Other Standards):

None at this time.

Questions for Data Request:

90-Day Notification Letter:

1. Provide a list of all XYZ Power Company (XYZ) BPS Facilities.
2. Provide a system one-line diagram for the XYZ system.

Data Request #1:

1. Provide the Facility Ratings for the following Facilities … (provide XYZ list of facilities determined in the Random Sampling of all XYZ facilities/elements).
2. Provide a station one-line diagram for the following XYZ substations …. (determined from Random Sample of facilities) .

LEAD SHEET TEMPLATE | APPENDIX C

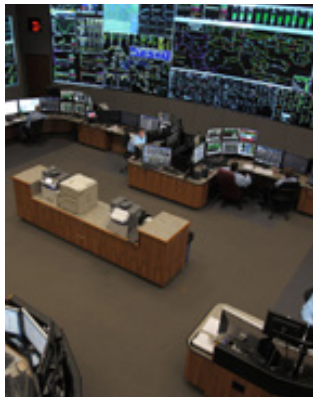
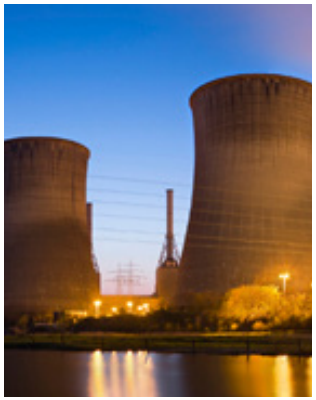
Preparation Inputs (PI):	Auditor / Analyst Commentary
Engagement Data	
Registered Entity:	
Entity Acronym:	
Entity NCR Number:	
Audit Review Type:	
Review / Engagement Date:	
Preparer:	
Date:	
Workpaper - RSAW Cross-Reference:	
Reviewer/Approval:	
Date:	
Source Population Type:	
Primary	
Dependent / Secondary	
Independent	
Other	
Obtain & Review Source Population(s) Record Layout:	
Identify Data Points, Field Values & Elements for Selection & Testing:	
Determine Alignment of Records History & Sampling Time Period:	
Validate Source Population(s) for Data Integrity & Completeness:	
Process Activities (PA):	
Standard	
Document the Sampling Testing Objective(s): [If applicable, Select the Testing Objective from the Requirements Menu]	
[If Applicable] - Other Testing Objective(s):	
Identify & Describe Impactful Risk [IRA] & Internal Control [ICE] Considerations:	
Select & Document Sampling Approach & Rationale: [If applicable, select Sampling Approach from the Menu]	
Comments and Rationale	
Determine the Initial Sampling & Size:	

Retention period noted in Standard:	
Document Relevant Time Periods Considered:	
Population Size	
Select Sample Size Based on Sampling Handbook Specifications, (Tables A), or Sampling Tool, (e.g., RAT-STATS)	
Document Statistical Sampling Metrics:	
(Table A Default Values)	
Confidence Level (95%)	
Margin of Error (10%)	
Random Seed Number	
Desired Precision Range (10%)	
Rate of Occurrence (0.5%)	
Comments for changes from default values	
Test Results Output (TRO)	
Assess & Document Test Sampling Results in Line with Stated Testing Objectives:	
Document if Sampling Approach Requires Expansion or Modification	
Document Basis for Expanded Sampling	
Document Basis for Deviations in Sampling or Planned Testing Procedures	
Determination/ Findings	
Area of Concerns	
Recommendation	

Click here to access the Lead Sheet Template that is posted on NERC's website.

ERO ENTERPRISE

Compliance Monitoring Competency Guide

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

VERSION 4 | 2018

PREFACE

This guide describes a systematic method for establishing and maintaining adherence to FERC Order 672 at 463 (18 CFR §39.7 (a)), which states, "The Electric Reliability Organization (ERO) and each Regional Entity (RE) shall have an audit program that provides for rigorous audits of compliance with Reliability Standards by users, owners and operators of the Bulk-Power System."

The purpose of the guide is not to definitively prescribe job descriptions. Rather, it identifies common levels of education and experience necessary to carry out high-quality compliance activities. The guide gives expectations that should be considered when developing specific Regional Entity job descriptions. It also contains the processes used to establish and determine employee skill sets and offers initial and continuing training requirements for electric reliability organization (ERO) Compliance Enforcement Authority (CEA) audit staff. It is a competency based training approach for promoting high-quality audits and consistency among RE CEA audit teams.

Compliance monitoring serves the foundational purpose of assuring that registered entities are complying with Reliability Standards. Further, compliance monitoring serves the public interest by providing necessary accountability and transparency in regard to compliance with mandatory standards. It also provides value and process improvement information, which allows registered entities to strengthen their operations. In this regard, the ERO Enterprise must have grounded principles and approaches whereby it acquires, develops and retains personnel to perform the compliance monitoring activity. This guide serves that purpose as well.

Role Expectations: Compliance personnel should provide both an objective analysis and the information needed for industry to make decisions necessary to improve the reliability of the bulk power system (BPS). The ability to perform high-quality audit work with competence, integrity, objectivity, and independence is based on an organization's ability to acquire, develop, and retain competent compliance personnel. A set of basic capabilities and competencies is necessary to produce a consistent product and approach across the ERO Enterprise.

Competency-Based Training: For the purposes of this handbook, the systematic approach to training (SAT) and competency-based training are interchangeable. The SAT includes five distinct, yet interrelated, phases. These phases include analysis, design, development, implementation, and evaluation. The SAT is consistent with other systematically based training systems, such as competency-based training, training system development (TSD), instructional systems development (ISD), and other similar methods. This guide applies the more classical concept and approach to systematically establishing training programs, with the focus of the document being primarily on the analysis phase. Beneficial comments (recommendations, additions, deletions) and any pertinent data that may be useful for improving this document should be addressed to: ComplianceOpsHelp@nerc.net.

AUTHORITATIVE GUIDANCE

CEA Staff Functional Roles

The following is a sampling of guidance pertaining to the ERO's drafting the Compliance Auditor Capabilities and Compliance Monitoring Competency Guide.

Rules of Procedure – Section 400 – Compliance Enforcement:

Section 401.4 - Role of Regional Entities in the Compliance Monitoring and Enforcement Program — "Each Regional Entity that has been delegated authority through a delegation agreement or other legal instrument approved by the Applicable Governmental Authority shall, in accordance with the terms of the approved delegation agreement, administer a Regional Entity Compliance Monitoring and Enforcement program to meet the NERC Compliance Monitoring and Enforcement Program goals and the requirements in this Section."

Section 403 - Each Regional Entity Compliance Monitoring and Enforcement Program shall promote excellence in the enforcement of Reliability Standards. To accomplish this goal, each Regional Entity Compliance Monitoring and Enforcement Program shall (i) conform to and comply with the NERC uniform Compliance Monitoring and Enforcement Program, Appendix 4C to these Rules of Procedure, except to the extent of any deviations that are stated in the Regional Entity's delegation agreement, and (ii) meet all of the attributes set forth in this Section 403."

Rules of Procedure – Appendix 4C:

Section 3.1 – "Compliance Audit processes for Compliance Audits conducted in the United States shall be based on professional auditing standards recognized in the U.S., which may include for example Generally Accepted Auditing Standards, Generally Accepted Government Auditing Standards and standards sanctioned by the Institute of Internal Auditors." All Compliance Audits shall be conducted in accordance with audit guides established for the Reliability Standards included in the Compliance Audit, consistent with accepted auditing guidelines as approved by NERC. The audit guides will be posted on NERC's website.

Section 3.1.5.1 – "The Compliance Audit team shall be comprised of members whom the Compliance Enforcement Authority has determined have the requisite knowledge, training and skills to conduct the Compliance Audit."

Section 403.5 – Regional Entity Compliance Staff: "Each Regional Entity shall have sufficient resources to meet delegated compliance monitoring and enforcement responsibilities, including the necessary professional staff to manage and implement the Regional Entity Compliance Monitoring and Enforcement Program."

AUTHORITATIVE GUIDANCE

CEA Staff Functional Roles (Cont.)...

Generally Accepted Government Accounting Standards

Chapter 1 – Government Auditing: Foundational and Ethical Principles

Chapter 3 – General Standards

Chapter 6 – Fieldwork Standards for Performance Audits

Institute of Internal Auditors – International Professional Practices Framework

Code of Ethics

Rules of Conduct

Attribute Standards

- 1100 – Independence and Objectivity
- 1200 – Proficiency and Due Professional Care

AUTHORITATIVE GUIDANCE

CEA Staff Compliance Training Requirements

FERC Order 672 at 463 (18 CFR §39.7 (a)) states, "The Electric Reliability Organization (ERO) and each Regional Entity (RE) shall have an audit program that provides for rigorous audits of compliance with Reliability Standards by users, owners and operators of the Bulk-Power System."

Section 402.9 of the NERC Rules of Procedure (ROP)[1] specifies, "NERC shall develop and provide training in auditing skills to all people who participate in NERC, RE Compliance Enforcement Audits (Audits), or both. Training for NERC and Regional Entity personnel and others who serve as Compliance Audit team leaders shall be more comprehensive than training given to industry subject matter experts and Regional Entity members. Training for Regional Entity members may be delegated to the Regional Entity."

The NERC Compliance Monitoring and Enforcement Program (CMEP) requires each audit team member to complete all NERC or NERC-approved auditor training applicable to the audit.[2]

In addition to the FERC orders and the NERC ROP, training and education is also addressed in the Regional Entity delegation agreements as follows: "NERC shall make available standardized training and education programs, which shall be designed taking into account input from <Regional Entities>, for <Regional Entity> personnel on topics relating to the delegated functions and related activities."[3]

PROFESSIONAL STANDARDS, ETHICAL PRINCIPLES AND RULES OF CONDUCT

The ERO and the Regional Entities (RE) (collectively the ERO Enterprise) ensure the reliability of the North American BPS through Appendix 4C of the NERC Rules of Procedure, the Compliance Monitoring and Enforcement Program (CMEP). Compliance Auditors fill the challenging role of evaluating the implementation of Reliability Standards, applying appropriate technical judgment, and effectively communicating to applicable parties the status and conclusions based on the work performed in support of this core responsibility. It is a Compliance Auditor's personal responsibility to adhere to a level of standards and principles that supports quality audits and to carry out his or her responsibilities in an effective and efficient manner.

[1] Effective January 30, 2014
[2] Rules of Procedure of the North American Electric Reliability Corporation, Appendix 4C, Section 3.1.5.2
[3] See Section 8b of the various Regional Delegation Agreements

PROFESSIONAL STANDARDS, ETHICAL PRINCIPLES AND RULES OF CONDUCT

The basis of the ERO Enterprise ethical principles and rules of conduct requirements are founded in the Generally Accepted Government Auditing Standards[4] (Yellow Book), specifically Chapters 1 and 3, and the Institute of Internal Auditors International[5] Professional Practices Framework (IIA-IPPF), specifically the Code of Ethics and the International Standards for the Professional Practice of Internal Auditing. Compliance Auditors are required to familiarize themselves with both resources. Compliance Auditors are expected to understand and demonstrate the following fundamental principles:

Integrity

The integrity of a Compliance Auditor is foundational to his or her use of professional judgment. Integrity is the way an auditor conducts his or her work, maintains an objective attitude, supports opinions with factual evidence, and remains free from biases.

Objectivity

Compliance Auditors must be free of conflicts[6] and base their work on facts. Objectivity must be maintained in the way auditors gather, evaluate, and communicate information. A Compliance Auditor must be free from conflicts of interest, in both fact and appearance, that affect impartiality and independence related to the entity or audit matter.

Confidentiality

The information, data, and documentation that a Compliance Auditor receives must be treated with a sense of ownership and must be protected from unnecessary exposure. Information collected by Compliance Auditors should not be disclosed without proper authority.[7]

Competency

A Compliance Auditor must possess the professional competence to complete his or her work. Competence is a function of an auditor's knowledge, skills, education, and experiences. A Compliance Auditor is expected to maintain and grow his or her professional competence through continuing education.

Professional Behavior

Compliance Auditors perform their work with honesty, diligence, integrity, and responsibility while avoiding conduct that may discredit the work of the ERO. Professional behavior requires Compliance Auditors to perform their duties in accordance with technical and professional standards.

---

[4] Link to the U.S. Government Accountability Office: http://www.gao.gov/products/GAO-12-331G
[5] Link to the IIA: https://na.theiia.org/Pages/IIAHome.aspx
[6] Rules of Procedure of the North American Electric Reliability Corporation, Appendix 4C, Section 3.1.5.2
[7] Rules of Procedure of the North American Electric Reliability Corporation, Section 1500

CEA COMPLIANCE AUDITOR ROLE EXPECTATIONS

Role Requirements and Qualifications

Professional standards require an audit team to collectively possess the knowledge, experience, education, and skills that allow the team to competently execute the audit. It is the ERO Enterprise's responsibility to identify the professional competence that is needed to perform the work in connection with the professional standards outlined in the previous section. REs should evaluate their organizations and determine the appropriate balance of education, experience, and background the audit team needs to perform its work in accordance with professional standards. Substituting years of experience for formal education is at the discretion of the RE. Professional competence is a combination of the combined education and experience of the individuals who comprise an audit team. Tables 1 and 2 provide guidance on how to to create a diverse team that collectively possesses the requisite skills to competently perform compliance activities.

Education and Certification

While the ERO does not specifically require levels of education or certification, REs should strongly consider blending educational backgrounds and certifications with professional experience. Table 1 outlines minimum expectations with regard to education and certification.

CEA COMPLIANCE AUDITOR ROLE EXPECTATIONS

Table 1 – Education and Certifications					
Education and Certifications		Auditor		LEAD	Manager
		O&P	CIP		
Education	**Graduate Degree:** MBA, Engineering, Information Systems, or similar technical discipline	N/A	N/A	N/A	p
	Bachelor's Degree: Electrical Engineering, Accounting, Auditing, Information Systems, or similar technical discipline	P	P	P	R
	Associate Degree: Electrical Engineering, System Operations, Information Systems, or similar technical discipline	A	A	A	N/A
Professional Certification	NERC-Certified system operator *(other certifications e.g. WECC, PJM)*	P	N/A	P	P
	Professional Engineer	P	N/A	P	P
	Auditor Certifications: Certified Internal Auditor, Certified Government Auditing Professional, Certified Quality Auditor, Certified Information Systems Auditor or similar	P	P	P	P
	Cyber and Physical Security: Certified in Risk and Information Systems Control, Certified Information Systems Security Professional, Certified Information System Manager, Physical Security Professional or similar	P	P	P	P

Legend		
R	Required	The Certification and Education is required for the Role, or justification for suitable substitution is necessary
P	Preferred	The possession of the Certification and Education impacts the success within the Role
A	Alternate	Will be considered in connection with years of experience and knowledge
N/A		Does not apply for the selected Role

CEA COMPLIANCE AUDITOR ROLE EXPECTATIONS

Continuing Education

Generally Accepted Government Auditing Standards (GAGAS) require auditors to maintain their professional competence through continuing professional education (CPE).[8] GAGAS requires Compliance Auditors to complete at least 24 hours of CPE every two years that directly relates to auditing.[9] Additionally, Compliance Auditors should obtain at least 56 additional CPE hours (a total of 80 hours of CPE in every two-year period) that enhance the Compliance Auditor's professional proficiency to perform audits.[10] A minimum of 20 CPE hours must be completed in each of the two years.[11] In addition to GAGAS, many professional societies both require and provide continuing education to maintain certifications like the ones indicated in Table 1. Continuing education hours taken to maintain such professional certification, as well as hours from relevant training offered by NERC or the REs, will count toward the continuing education requirement. Both NERC and RE workshops with hours specifically dedicated to furthering audit knowledge and technical competencies will count toward requisite training requirements.

It is the RE's responsibility to develop a system for tracking and monitoring educational hours obtained by Compliance Auditors.

Industry Knowledge and Experience

A combination of knowledge and experience allows an auditor to make professional judgments in an educated manner. Practical experiences *(outlined in Table 2)* are necessary for auditors to competently execute the technical aspects of their roles. Blending Compliance Auditors' technical and audit knowledge within audit teams is necessary for the ERO Enterprise to effectively carry out its collective responsibility. Table 2 is not exhaustive, nor are auditors expected to be proficient in each area. The table provides guidance on the types of knowledge and experience that support the creation of professionally competent audit teams. An individual's knowledge and experience is assessed relative to his or her demonstrated level of capability and competency. The Individual Core Competency and Professional Competency matrices beginning on 200 of this document should be referenced accordingly.

[8] GAO-12-331G, Section 3.76
[9] Id
[10] Id
[11] Id

CEA COMPLIANCE AUDITOR ROLE EXPECTATIONS

Table 2 – Knowledge and Experience

Knowledge and Experience		Auditor		LEAD	Manager	Audit Team
		O&P	CIP			
Operational & Technical	Bulk Electric System (BES) operation, design, planning, or analysis	P	P	P	p	R
	FERC/NERC/Nuclear Regulatory Commission knowledge	P	P	R	R	R
	Transmission Systems: • Operation - real-time studies, and near-term planning • Design - transmission planning/operation • Modeling and studies - steady state, dynamic, transient, short circuit, etc.	P	P	P	P	R
	Generation: 1. Balancing of load and demand 2. Power plant fundamentals 3. Equipment knowledge *(relays, generator types, breakers)*, Protection System Design, maintenance and testing, engineering	P	P	P	P	R
	Reliability Coordination: 1. Wide area power systems operation and control 2. Functional relationship roles and responsibilities	P	P	P	P	R
	Substation design	P	P	P	P	R
	EMS/SCADA engineering	P	P	P	P	R
	Communication systems	P	P	P	P	R
	Protection system design, maintenance and testing	P	P	P	P	R
	Operating systems, databases, network architecture/application	P	R	R	P	R
	Physical security approaches and systems		P	P	P	R
	Seasonal assessment studies—near and long term	P		P	P	R

Legend		
R	Required	The Certification and Education is required for the Role, or justification for suitable substitution is necessary
P	Preferred	The possession of the Certification and Education impacts the success within the Role
A	Alternate	Will be considered in connection with years of experience and knowledge
N/A		Does not apply for the selected Role

CEA COMPLIANCE AUDITOR ROLE EXPECTATIONS

Table 2 – Knowledge and Experience (Cont.)...

Knowledge and Experience		Auditor		LEAD	Manager	Audit Team
		O&P	CIP			
Operational & Technical	Cyber Security		R	P	p	R
	Vulnerability assessments		R	P	P	R
Audit	Knowledge of GAGAS and IIA Professional Practices	R	R	R	R	R
	Sampling knowledge—both statistical and nonstatistical	R	R	R	R	R
	Experience developing and performing risk assessments	R	R	R	R	R
	Strong ability to document, assess and test controls	R	R	R	R	R
	Testing of data, processes and controls	R	R	R	R	R
	Planning, performing and reporting audit work	R	R	R	R	R
	Risks and controls for information systems	P	R	R	R	R
	General network security		R	R	P	R

Legend		
R	Required	The Knowledge and Experience is required for the Role *(required within each audit team as applicable for the scope of each audit)*
P	Preferred	The possession of the Knowledge and Experience impacts success within the Role

ROLE EXPECTATIONS AND RESPONSIBILITIES

Continuing Education

Role expectations and responsibilities identify essential tasks and activities that are assigned to a specific position. It is the RE's responsibility to develop appropriately titled and scoped roles. The identified tasks and activities may be assigned to different roles or areas within the organization as needed by the RE.

Operational and Critical Infrastructure Protection (CIP) Compliance Auditor

Role Expectations

The Compliance Auditor works with the Audit Team, Audit Team Lead (ATL), Compliance Audit Manager (Manager), and/or others as required to understand risk, audit scope, and expectations for the execution of test plans in connection with compliance activities. The Compliance Auditor is assigned to a schedule of compliance activities for which he or she will follow ERO Enterprise compliance audit guidance as well as GAGAS and the IIAIPPF. The Compliance Auditor uses fundamental operational and technical skills to support the ERO Enterprises objectives related to the reliability of the BES.

The Compliance Auditor performs audits of registered entities, understands and evaluates controls, and validates the functioning of controls through substantive testing of records and data in order to verify compliance with Reliability Standards and their related requirements. The Compliance Auditor prepares and reviews documentation, workpapers, interview summaries, and findings with the ATL. The Compliance Auditor may also perform additional functions and activities, such as spot checks, evaluations of self-certifications, and reviews of data submittals from registered entities. The Compliance Auditor works under direct supervision of the ATL.

Role Responsibilities

The Compliance Auditor is responsible for both audit and non-audit activities as outlined in Table 3 *(on the next page)*:

ROLE EXPECTATIONS AND RESPONSIBILITIES

Table 3 – Compliance Auditor Responsibillities

Task	Activity	Function	
		O&P	CIP
Audit	Work with audit team and ATL in risk assessment to appropriately scope audits	✓	✓
	Understand assigned Reliability Standards and audit assignments	✓	✓
	Understand, document, and evaluate systems of internal control and appropriately test for design and function	✓	✓
	Execute test plans within the scope of the audit *(e.g., use of Reliability Standard Audit Worksheets (RSAWs) and other audit tools)*	✓	✓
	Review, test, and assess data for compliance with Reliability Standards	✓	✓
	Conduct and document discussions with registered entity personnel	✓	✓
	Appropriately secure data and information in accordance with all applicable policies	✓	✓
	Work with computerized information systems to extract and analyze information	✓	✓
	Draft and communicate findings to the lead auditor throughout the audit	✓	✓
	Develop and produce work papers that support audit results	✓	✓
	Achieve goals within established time and constraints	✓	✓
General	Ensure personal travel arrangements are made for audit engagements	✓	✓
	Mentor peers on audit techniques as well as operational and technical knowledge	✓	✓
	Assist with the development and delivery of training	✓	✓
	Review changes to Reliability Standards and Regional and NERC policies for impact on audit	✓	✓

The RE is responsible for further defining role expectations that may describe additional duties and functions.

ROLE EXPECTATIONS AND RESPONSIBILITIES

Lead Compliance Auditor

Role Expectations

The Compliance Audit Lead (Lead) works with the Manager to plan and execute audit objectives. The Lead is responsible for ensuring the audit team understands and follows ERO Enterprise compliance audit guidance, as well as GAGAS and the IIA-IPPF. He or she uses advanced operational and technical skills to support the ERO Enterprise's objectives related to the reliability of the Bulk Electric System (BES).

The Lead is responsible for working with and directing the audit team in the execution of audit activities. In addition to auditing controls and testing data, the Lead works with the audit team to prepare and review documentation, work papers, interview summaries, and findings with the Manager. The Lead works under direct supervision of the Manager. Additionally, he or she will also manage and perform activities related to conducting spot checks, evaluating self-certifications, and reviewing data submittals from registered entities.

Role Responsibilities

The Lead is responsible for both audit and non-audit activities as outlined in Table 4 *(on the next page)*:

ROLE EXPECTATIONS AND RESPONSIBILITIES

Table 4 – Lead Compliance Auditor Responsibilities

Task	Activity
Audit	Manage the planning, execution and completion of registered entity audits
	Schedule and conduct planning meetings with audit team
	Verify and communicate travel schedules with the audit team
	Manage activities related to the assessment of the registered entity's risk and recommend audit scope
	Conduct meetings with the registered entity Primary Compliance Contact (PCC)
	Schedule and manage opening, status of and closing meetings with the registered entity
	Assign scoped Reliability Standards to team members and review audit testing approach
	Verify the audit team completed its assigned tasks in an appropriate time frame
	Understand, document, and evaluate systems of internal control and appropriately test for design and function
	Monitor the execution of audit test plans within the scope of the audit
	Ensure audit team understands how to appropriately secure data and information in accordance with policies
	Review interviews, testing, and findings with the audit team throughout the audit
	Review and approve modifications to audit scope and testing
	Review and approve work papers that support audit results
	Review and edit the audit report for submission to the registered entity, NERC and FERC
	Meet with Enforcement and/or Registration to discuss audit findings
General	Coach audit team members on audit techniques as well as operational and technical knowledge
	Develop and deliver training on audit and regulatory concepts
	Review changes to Reliability Standards and policies for impact on audit
	Meet with audit manager and auditors to discuss performance feedback

The RE is responsible for further defining role expectations that may describe additional duties and functions.

ROLE EXPECTATIONS AND RESPONSIBILITIES

Compliance Audit Manager

Role Expectations

The Manager works with senior management and other regional experts to assess regional risk, develop annual audit plans, evaluate and determine resource and budgetary needs, and assign audits to Lead Auditors. The Manager is responsible for ensuring that the audit team understands and follows ERO Enterprise compliance audit guidance, as well as GAGAS and the IIA-IPPF. The Manager uses expert operational and technical skills to support the ERO Enterprise's objectives related to the reliability of the BES.

The Manager is responsible for directing multiple audits and audit teams in both understanding registered entity risk and scoping and executing audits. He or she directs efforts related to planning and executing individual audit objectives, including the review and sign-off of work papers, audit reports, and other formal documentation. The Manager also directs activities related to conducting spot checks, evaluating self-certifications, and reviewing data submittals from registered entities.

Role Responsibilities

The Manager is responsible for both audit and non-audit activities as outlined in Table 5 *(on the next page)*:

ROLE EXPECTATIONS AND RESPONSIBILITIES

Table 5 – Compliance Audit Manager Responsibilities

Task	Activity
Audit	Work with senior management to develop the annual audit plan (CMEP-IP)
	Develop the audit schedule and review audit resources to assure the completion of the plan
	Review the audit schedule with ATLs and assign audit activities
	Meet with the ATL to determine appropriate staffing levels and competencies for audit activities
	Report the execution of the audit plan and disclose any issues to senior management
	Meet with the ATL to determine and set the scope for individual audits
	Approve the final audit scope and test plan
	Review and discuss budget with the ATL for audits at the beginning and end of audits
	Conduct regular meetings with the ATLs to discuss audit planning, execution, findings, etc.
	Perform select reviews of audit work to verify completion
	Meet with registered entity management as needed
	Sign off on audit work papers, final reports, performance assessments, etc.
	Discuss audit observations with FERC and NERC as needed
	Report back to management end-of-year results, lessons learned, and process improvements
General	Mentor peers on audit techniques as well as operational and technical knowledge
	Assist with the development and delivery of training
	Review changes to Reliability Standards and policies for impact on audit
	Provide feedback on Reliability Standards based on audit experiences
	Assure annual staffing needs are met and perform interviews of audit candidates
	Develop and deliver training at auditor workshops
	Meet with registered entities to provide training on risk, controls and compliance
	Meet with NERC on a routine basis to discuss compliance activities
	Participate in ERO Enterprise initiatives and projects
	Coordinate compliance activities with other Regional Entities as required

The RE is responsible for further defining role expectations that may describe additional duties and functions.

INDIVIDUAL CORE & PROFESSIONAL COMPETENCY MATRIX

Core Competencies are the primary strengths auditors use to effectively perform assigned work. Individuals possess varying levels of competencies that allow the ERO Enterprise to pool the knowledge and collectiventechnical capacities to produce high-quality compliance audit work. An audit team must possess a combined level of individual Core and Professional Competencies that allow the audit team to competently execute each audit.

In addition to the knowledge and experience noted in the Table 2, individuals should also possess professional competencies. Professional competencies are specific experiences and technical competencies that when combined with core competencies create a higher level of expertise. Technical backgrounds are not expected to be consistent, nor is there an expectation of equal knowledge across all aspects of the ERO Enterprise regulatory responsibilities. As noted below, individuals are expected to have or obtain the specified level of expertise in one or more families of Reliability Standards. It is not expected or required that each compliance auditor understand or demonstrate the competency level for each Reliability Standard family.

INDIVIDUAL CORE & PROFESSIONAL COMPETENCY MATRIX

Table 6 – CEA Staff Compliance Roles

Family	Competency	Attribute	Functional Roles		
			Auditor	Lead	Manager
Foundational Competencies	Interpersonal	Conflict Management	○	◐	●
		Ethics and Values	◐	◐	●
		Teamwork	○	◐	◐
	Communications	Business, Legal, and Technical Writing	○	◐	◐
		Interviewing and Conversations	○	◐	◐
		Presentation	○	◐	◐
		Listening	◐	◐	◐
	Functional & Technical	Time Management	○	◐	◐
		Technology	○	◐	◐
		Auditing	○	◐	●
		General Engineering, Operational and Technical	○	◐	◐
	Management	Directing Others		○	●
		Organization	○	◐	●
		Leadership		○	●
		Team Building		○	●

Symbol Key		
Icon	Level	Description
○	Basic to Intermediate	Sufficient to broad understanding of the competency, demonstrating intermediate required skills and proactive execution
◐	Intermediate to Advance	Extensive understanding of the competency, demonstrating advanced required skills, proactive execution advanced leadership by example
●	Advanced to Expert	Complete understanding of the competency, demonstrating expert required skills, proactive execution, and leadership by example and by fostering the vision and environment

INDIVIDUAL CORE & PROFESSIONAL COMPETENCY MATRIX

Table 6 – CEA Staff Compliance Roles (Cont.)...

Family	Competency	Attribute	Functional Roles		
			Auditor	Lead	Manager
Audit Competencies	Audit Fundamentals	Documentation Expectations and Management	○	◐	●
		Professional Development	◐	◐	●
		Audit Resources, Tools and Guidance	○	◐	◐
	Audit Cycle	Audit Planning	○	◐	◐
		Audit Fieldwork	○	◐	◐
		Audit Reporting	○	◐	◐
	Audit Oversight	Managing On-site Visits	◐	◐	◐
		Communications with Registered Entities	○	◐	◐
		Auditing	○	◐	◐
		Quality Assurance	○	◐	●

Symbol Key

Icon	Level	Description
○	Basic to Intermediate	Sufficient to broad understanding of the competency, demonstrating intermediate required skills and proactive execution
◐	Intermediate to Advance	Extensive understanding of the competency, demonstrating advanced required skills, proactive execution advanced leadership by example
●	Advanced to Expert	Complete understanding of the competency, demonstrating expert required skills, proactive execution, and leadership by example and by fostering the vision and environment

INDIVIDUAL CORE & PROFESSIONAL COMPETENCY MATRIX

Table 6 – CEA Staff Compliance Roles (Cont.)...

Family	Competency	Attribute		Functional Roles		
				Auditor	Lead	Manager
NERC Specific Skills	Enforcement	Conflict Management		○	◐	●
		Ethics and Values		○	◐	●
	Industry & Regulatory Knowledge	Bulk Power System Fundamentals		○	◐	●
		Legal Aspects - FERC, Regulations, Rules, Governance		○	◐	●
		NERC Functional Model		○	◐	●
	Reliability Standards *(Specialty in one or more area)*	**BAL**	Resource and Demand Balancing	○	●	◐
		CIP	Critical Infrastructure Protection	○	●	◐
		COM	Communication	○	●	◐
		EOP	Emergency Preparedness and Operations	○	●	◐
		FAC	Facilities Design, Connections and Maintenance	○	●	◐
		INT	Interchange Scheduling and Coordination	○	●	◐
		IRO	Interchange Reliability Operations and Coordination	○	●	◐
		MOD	Modeling, Data, and Analysis	○	●	◐
		NUC	Nuclear	○	●	◐
		PER	Personnel Performance, Training and Qualifications	○	●	◐
		PRC	Protection and Control	○	●	◐
		TOP	Transmission Operations	○	●	◐
		TPL	Transmission Planning	○	●	◐
		VAR	Voltage and Reactive	○	●	◐

Symbol Key

Icon	Level	Description
○	Basic to Intermediate	Sufficient to broad understanding of the competency, demonstrating intermediate required skills and proactive execution
◐	Intermediate to Advance	Extensive understanding of the competency, demonstrating advanced required skills, proactive execution advanced leadership by example
●	Advanced to Expert	Complete understanding of the competency, demonstrating expert required skills, proactive execution, and leadership by example and by fostering the vision and environment

COMPETENCY DEFINITIONS

Competencies are the behaviors that encompass the knowledge, attitudes, motives, and skills that distinguish excellent performance. Individual and organizational success relies on a set of competencies that:

- Establish fair, uniform, and consistent criteria for decision making;
- Establish a common language for defining success across the ERO Enterprise; and
- Reinforce the ERO Enterprise unique culture.

The core set of competencies identified in the preceding tables are defined below.

Individual Core Competencies

Interpersonal: Life skills used every day to interact with other people both individually and in groups.

Conflict Management – Steps up to conflicts, seeing them as opportunities; reads situations quickly; good at focused listening; can hammer out tough agreements and settle disputes equitably; can find common ground and promote cooperation with minimal disruption.

Ethics and Values – Adheres to an appropriate and effective set of core values and beliefs during both smooth and difficult times; acts in line with those values; rewards the right values and disapproves of others. Understands the requirements outlined in GAGAS and IIA-IPPF.

Teamwork – Quickly finds common ground and solves problems for the good of all; represents his/her own interests yet is fair to teams; solves problems with peers with minimal disruption; is seen as a team player and is cooperative; easily gains trust and support of peers; encourages collaboration; can be candid with peers.

Communications: Methods used to convey and receive information to achieve a desired effect.

Business and Technical Writing – Able to write clearly and succinctly in a variety of communication settings and styles; can get messages across that prompt appropriate action.

Interviewing and Conversations – Conducts discussions in a manner that puts people at ease and builds constructive dialogue. Appropriately plans for conversations through preparation and breadth of questions. Maintains an objective attitude during discussions that are intended to obtain facts in support of audit objectives.

COMPETENCY DEFINITIONS

Individual Core Competencies (Cont.)...

Presentation Skills – Effective in a variety of formal and informal presentation settings: one-on-one, small and large groups, or with peers, direct reports, and bosses; is effective both inside and outside the organization, on both current data and controversial topics; commands attention and can manage group dynamics; can change tactics midstream when necessary.

Listening Skills – Practices attentive and active listening; has patience to hear people out; can accurately restate the opinions of others even when in disagreement.

Functional & Technical: Industry background and technical knowledge and skills to perform role at a high level of accomplishment.

Time Management – Uses time effectively and efficiently; values time; concentrates efforts on priorities; gets more done in less time than others; can attend to a broader range of activities.

Technology – Able to select and apply contemporary forms of technology to solve problems or compile information. Has knowledge of and uses MS Office products; is familiar with audit management tools, as well as governance, risk, and compliance applications; has experience using technology to analyze information or data; has experience using technology as venue for information sharing. Able to determine which technologies apply to the task and understand the limitations of those technologies.

Auditing – Understands the role of an independent compliance auditor and demonstrates consistent execution of quality by adhering to professional standards and ERO Enterprise guidance; exercises sound professional judgment, objectivity, and skepticism.

General Engineering, Operational, and Technical – Uses professional experience and continuing education to accurately and appropriately assess data and information to support conclusions made through audit engagements.

Management: Management skills necessary to lead organizational strategy, drive activities, and develop audit staff.

Directing Others – Establishes clear directions; sets stretching objectives; distributes the workload appropriately; lays out work in a well-planned and organized manner; maintains two-way dialogue with others on work and results; brings out the best in people; is a clear communicator.

COMPETENCY DEFINITIONS

Individual Core Competencies (Cont.)...

Organization – Marshals resources *(people, funding, material, and support)* to get things done; can orchestrate multiple activities at once to accomplish a goal; uses resources effectively and efficiently; arranges information and files in a useful manner.

Leadership – Leads people toward meeting the ERO Enterprise's vision, mission, and goals; provides an inclusive workplace that fosters the development of others; facilitates cooperation and teamwork; supports constructive resolutions to conflict.

Team Building – Blends people into teams when needed; creates strong morale and spirit in teams; shares wins and successes; fosters open dialogue; lets people finish and be responsible for their work; defines success in terms of the whole team; creates a feeling of belonging in the team.

Audit Fundamentals: Professional level understanding of audit procedures to ensure engagements are appropriately conducted.

Documentation Expectations and Management – Documents, backs up, and archives all work fully and accurately to comply with ERO Enterprise standards and other guidance as reflected in auditor tools and resources.

Professional Development – Maintains and develops audit skills and knowledge/expertise of audit methodologies and tools by participating in formal and informal learning activities, including active participation in engagementspecific learning activities; applies audit methodologies and relevant audit requirements to work in assigned areas of audit engagements.

Audit Resources, Tools, and Guidance – Consistently uses auditor resources, tools, and guidance on work in assigned areas of audits *(e.g., Auditor Handbook, risk and controls assessment tools and methodologies, sampling techniques, RSAWs)*.

Audit Cycle: Professional understanding of the elements of a complete compliance audit activity and how each is accomplished in accordance with the Auditor Checklist.

Audit Planning – Understands and executes the tasks outlined in the Auditor Checklist, including gathering data, assessing risk, determining scope, developing test plans, communicating activities, and preparing for the execution of testing.

COMPETENCY DEFINITIONS

Individual Core Competencies (Cont.)...

Audit Fieldwork – Understands and executes the tasks outlined in the Auditor Checklist; for assigned areas of the audit engagement: exercises professional skepticism and asks questions to identify and respond to audit risks, identifies auditing issues for consideration by CEA management, understands the information that is provided, and works with the audit team to test the information for accuracy and completeness.

Audit Reporting – Understands and executes the tasks outlined in the Auditor Checklist; applies knowledge of relevant Reliability Standards to work on engagements and resolves issues with registered entity management; competently uses the audit report template; understands techniques to assure the creation of a defensible audit report; executes on retention practices.

Audit Oversight:

Managing On-Site Visits – Manages the processes related to visiting a registered entity *(e.g., coordinating travel and logistics, scheduling interviews, ensuring staff preparation, etc.)*.

Communications with Registered Entities – Manages contact with the registered entity's compliance contact and management as required, ensuring the understanding of the audit process and related activities. Delivers timely status updates and appropriately communicates needs and findings.

Quality Assurance – Understands and executes the tasks outlined in the Auditor Checklist; understands the meaning of 1) Quality Assurance, 2) common audit weaknesses, 3) embedding quality assurance into audit processes and tools, and 4) implementing quality improvements.

COMPETENCY DEFINITIONS

Individual Professional Competencies

Enforcement:

Enforcement Processes (e.g., Find, Fix, and Track) – Understands auditor role in enforcement processes; applies guidance as it relates to audit findings; stays current with initiatives to streamline enforcement processes.

Processing of Potential Violations – Understands how compliance audit activities, testing, data collection, evaluation, and documentation support the processing of potential violations; communicates effectively with enforcement staff to process potential violations.

Industry and Regulatory Knowledge:

Bulk Power System Fundamentals – Understands the fundamentals and structure of the bulk power system: interconnected power system operations; generation and power plant characteristics; transmission; substation and system protection; control center operations; and other basic components of the bulk power system.

Legal Aspects – Understands basic principles related to the ERO's legal authority to enforce Reliability Standards, the structure of the ERO, and duties delegated to the Regional Entities.

NERC Functional Model – Demonstrates knowledge of the functions that must be performed to ensure reliability of the bulk electric system; applies Functional Model as the foundation and framework of Reliability Standards.

Reliability Standards:

General Understanding by Standards Family – Understands how to apply Reliability Standards and requirements to the specified function and task for the registered entity being audited. Demonstrates familiarity with the language of the Reliability Standards and requirements, technical aspects of the standard and requirement, and processes for compliance with standards and requirements, including the technical apects of the RSAW. It is not expected or required that each compliance auditor understand or demonstrate competency for each Reliability Standard. The audit team should possess the collective requisite knowledge to audit the Reliability Standards that have been scoped for a specific audit.

TRAINING APPROACH

In the analysis phase of an SAT, one must identify and list the duties of a job. The tasks that must be done to accomplish these identified duties are then analyzed. Many of the tasks are so large that they are broken into smaller parts called task elements. The knowledge, skills, and attitudes needed to successfully perform the task are determined from the tasks and elements.

After the tasks are identified, they are reviewed and characterized by difficulty, importance, and frequency to help determine whether training is required prior to performing the task. These task groupings also aid in the selection of individual tasks on which auditors or staff will receive continuing or sustainment training throughout their careers. A more difficult task would potentially have more training associated with it than an easy or more routine task, which may not have formal training but may only have a procedure for the auditor to follow.

The outcome of the analysis phase is a task analysis that lists the tasks that are performed to accomplish the duties of a position and the knowledge, skills, and attitudes necessary to perform the tasks.

The involvement of management is important to the analysis process. Trainers should not be expected to know everything about a job and they do not set the performance expectations. Setting performance expectations is the responsibility of the operating group. The operating group must provide their goals and expectations for student performance to the trainers during the analysis phase. The trainer will use these goals and expectations for successful work performance to create the criteria for completing the training course.

Users of this Guide should consider the variety of training options that are available for establishing and maintaining personnel training and qualification programs. Blending classical and alternative systematic approaches to training methods often yields the most effective product. Users should emphasize the fundamental goal of any training program as they use this guideline—the goal is to prepare auditors to do their jobs safely, efficiently, and effectively. This Guide is the first step in designing and implementing training programs that meet these requirements and expectations.

The determination of initial and continuing training needs for ERO compliance auditors is guided by the ERO Staff Training Group (STG) and the NERC Training and Education Department, in conjunction with the NERC Compliance Department. The STG's charter[12] is to develop and coordinate delivery of training and related education to NERC and RE staff to effectively carry out delegated functions.

[12] ERO Staff Training Group Charter, April 2013

TRAINING APPROACH

The STG will use this Guide, along with any direction from management, to oversee an SAT for ERO Compliance Auditors. A common competency-based training approach will promote quality and consistency across the ERO by establishing a solid foundation of knowledge and skills, while considering RE-specific differences in implementation.

The STG uses a six-step framework in making decisions for the development and delivery of ERO staff training.

The steps are:

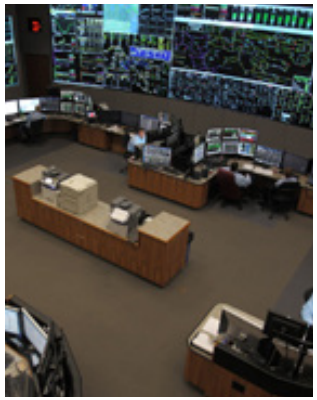
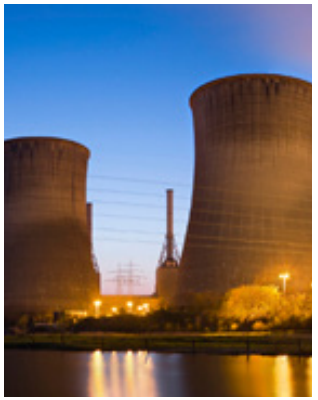
1. Identify audience
2. Identify training needs
3. Prioritize training needs
4. Determine development and delivery methods
5. Evaluate training materials
6. Sustain curriculum.[13]

NERC and the REs are not expected to sponsor training on all identified competencies in all years. The STG, NERC, and the REs will use the framework above to determine the appropriate curriculum on an ongoing basis. REs are responsible for ensuring individuals serving in all compliance audit functional roles either have the qualifications or receive appropriate training in the identified core and professional competencies. Appropriate training may include on-the-job training, NERC-sponsored training, RE-sponsored training, or other instructor-led or e-learning training.

[13] ERO Staff Training Decision Framework, January 22, 2014

ERO ENTERPRISE

Risk-Based Enforcement

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

VERSION 4 | 2018

RISK-BASED ENFORCEMENT | TABLE OF CONTENTS

RISK-BASED ENFORCEMENT

Background

In the United States, the ERO Enterprise's enforcement jurisdiction is drawn from the Energy Policy Act of 2005 (the Act), which added section 215 to the Federal Power Act (FPA). Section 215 made compliance with electric Reliability Standards mandatory and authorized the creation of an ERO and Regional Entities to establish and enforce Reliability Standards. Under section 215(e)(1) of the FPA, NERC or a Regional Entity may impose a penalty on a user, owner, or operator of the bulk power system (BPS) for a violation of a Reliability Standard approved by FERC. The ERO Enterprise also has compliance monitoring and enforcement responsibilities in Canada and part of Mexico. Enforcement activities in those jurisdictions follow the laws and regulations of the Applicable Governmental Authorities.

As the ERO, NERC has set forth Sanction Guidelines outlined in its Rules of Procedure that govern the ERO Enterprise's penalties and non-monetary sanctions for Reliability Standard violations. This document provides information on the ERO Enterprise's enforcement philosophy, i.e., the ERO Enterprise's approach for assessing and resolving noncompliance while working toward a shared goal of improving the reliability of the BPS.

ERO Enterprise Core Values and Guiding Principles

The ERO Enterprise's Strategic Plan[1] promotes the ERO Enterprise's core values and guiding principles, which are based on accountability and independence, responsiveness, fairness and inclusiveness, adaptation and innovation, excellence, efficiency, and integrity. These core values and guiding principles support the four pillars of the ERO Enterprise's efforts, namely, reliability, assurance, learning, and a risk-based approach.

Strategic Goals Related to Enforcement

Strategic goal 2 provides that the ERO Enterprise shall:

Be a strong enforcement authority that is independent, without conflict of interest, objective and fair, and promote a culture of reliability excellence through risk-informed compliance monitoring and enforcement. The ERO Enterprise retains and refines its ability to use Reliability Standards enforcement when warranted and imposes penalties and sanctions commensurate with risk.

The risk-based enforcement approach allows for the appropriate allocation of resources to the issues that pose a higher level of risk to the reliability of the BPS.

RISK-BASED ENFORCEMENT

ERO Enterprise Core Values and Guiding Principles (Cont.)...

Guiding Enforcement Principles

The following principles serve as guidelines for the conduct and behavior of all involved in the ERO Enterprise enforcement program to ensure alignment with strategic goal 2 and the ERO Enterprise's core values.

Compliance Enforcement Authorities are independent, without conflict of interest, objective and fair.

The ERO Enterprise strives to be a strong enforcement authority that is independent, without conflict of interest, objective, and fair. NERC and each of the Regional Entities has a code of conduct addressing the professional and ethical standards applicable to its personnel. Foremost among these standards is the requirement that no person work on a matter where that work may affect the person's financial interest. The ERO Enterprise also expects its personnel to conduct themselves professionally and respectfully when engaging with registered entities or other stakeholders. Personnel who do not meet these standards are subject to discipline, up to and including termination.

Enforcement program promotes culture of reliability excellence through a risk-based approach.

The ERO Enterprise's risk-based enforcement philosophy generally advocates reserving enforcement actions under section 5.0 of the Compliance Monitoring and Enforcement Program for those issues that pose a higher risk to the reliability of the BPS. The risk of a noncompliance is determined based on specific facts and circumstances, including any internal controls in place at the time of the noncompliance. The ERO Enterprise works with registered entities to ensure timely remediation of potential risks to the reliability of the BPS and to prevent recurrence of the noncompliance. The enforcement process allows parties to address risks collaboratively and promote increased compliance and reliability through improvement of programs and controls at the registered entities.

For issues posing a minimal risk, NERC and the Regional Entities may exercise appropriate judgment whether to initiate a formal enforcement action or resolve the issue outside of the formal enforcement processes. The availability of streamlined treatment of minimal risk noncompliance outside of the formal enforcement process encourages self-inspection and prompt mitigation of issues by registered entities.

For registered entities with demonstrated internal controls who are permitted to log minimal risk noncompliance, the ERO Enterprise applies a presumption of non-enforcement treatment of such minimal risk noncompliance. Registered entities are encouraged to establish robust internal controls for the identification, assessment, correction, and prevention of noncompliance.

RISK-BASED ENFORCEMENT

ERO Enterprise Core Values and Guiding Principles (Cont.)...

Use of streamlined processes allows the ERO Enterprise to oversee the activities of registered entities in a more efficient manner and to focus resources where they result in the greatest benefit to reliability. In this context, efficiency does not necessarily mean less time or effort. Rather, it is using the requisite time, knowledge, and skills required for each circumstance. In addition, this approach allows the ERO Enterprise to continue to provide clear signals to registered entities about identified areas of concern and risk prioritization, while maintaining existing visibility into potential noncompliance and emerging areas of risk. Outcomes for noncompliance are based on the risk of a specific noncompliance and may range from streamlined, non-enforcement processes, to significant monetary penalties or sanctions.

Enforcement actions are used and penalties are imposed when warranted, commensurate with risk.

An element of a risk-based approach to enforcement is accountability of registered entities for their noncompliance. No matter the risk of the noncompliance, the registered entity still bears the responsibility of mitigating that noncompliance and working to prevent recurrence. Based on the risk, facts, and circumstances associated with that noncompliance, the Regional Entity decides on an appropriate disposition track, inside or outside of an enforcement action, as described above, and whether a penalty or sanction is appropriate for the noncompliance.

Penalties and sanctions are generally warranted for some moderate risk violations and most, if not all, serious risk violations *(e.g., uncontrolled loss of load, CIP program failures)* and when repeated noncompliance may constitute an aggravating factor. In addition to the use of penalties to deter undesired behavior, the ERO Enterprise also encourages desired behaviors.[1] Specifically, Regional Entities may offset penalties to encourage valued behavior. Factors that may mitigate penalty amounts include registered entity cooperation, accountability *(including admission of violations)*, culture of compliance, and self-reporting of noncompliance.

Regional Entities may also grant credit in enforcement determinations for certain actions undertaken by registered entities for improvements that increase reliability and/or security in addition to the mitigating factors mentioned above. For example, Regional Entities may consider significant investments in tools, equipment, systems, or training made by registered entities, beyond those otherwise planned and required for compliance/mitigation, as an offset for proposed penalties in enforcement determinations. Regional Entities do not award credits or offsets for actions or investments undertaken by a registered entity that are required to mitigate the noncompliance.

[1] The Sanction Guidelines, Appendix 4B to the NERC Rules of Procedure, in alignment with Section 215, establish a general rule that penalties and sanctions imposed for the violation of a Reliability Standard shall bear a reasonable relation to the seriousness of the violation while also reflecting consideration of the other factors specified in the Sanction Guidelines. The Sanction Guidelines are available at http://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix_4B_SanctionGuidelines_20140701.pdf

RISK-BASED ENFORCEMENT

ERO Enterprise Core Values and Guiding Principles (Cont.)...

NERC engages in regular oversight of Regional Entity enforcement activities to confirm that the Regional Entities have followed the CMEP. This oversight evaluates the consistency of disposition methods, including assessment of a penalty or sanction, with previous resolutions of similar noncompliance involving similar circumstances. The NERC Board of Trustees Compliance Committee (the Compliance Committee) considers the recommendations of NERC staff regarding approval of Full Notices of Penalty and monitors the handling of noncompliance through the streamlined disposition methods of Spreadsheet NOPs, FFTs, and Compliance Exceptions.

Actions are timely and transparent.

The ERO Enterprise maintains transparency regarding enforcement matters. NERC's Rules of Procedure *(including the CMEP and Sanction Guidelines)* and program documents are available to the public.[2] NERC also posts information on enforcement actions on a monthly basis.[3] Moreover, information on the efficiency of the enforcement program is available to the public on a quarterly basis.[4]

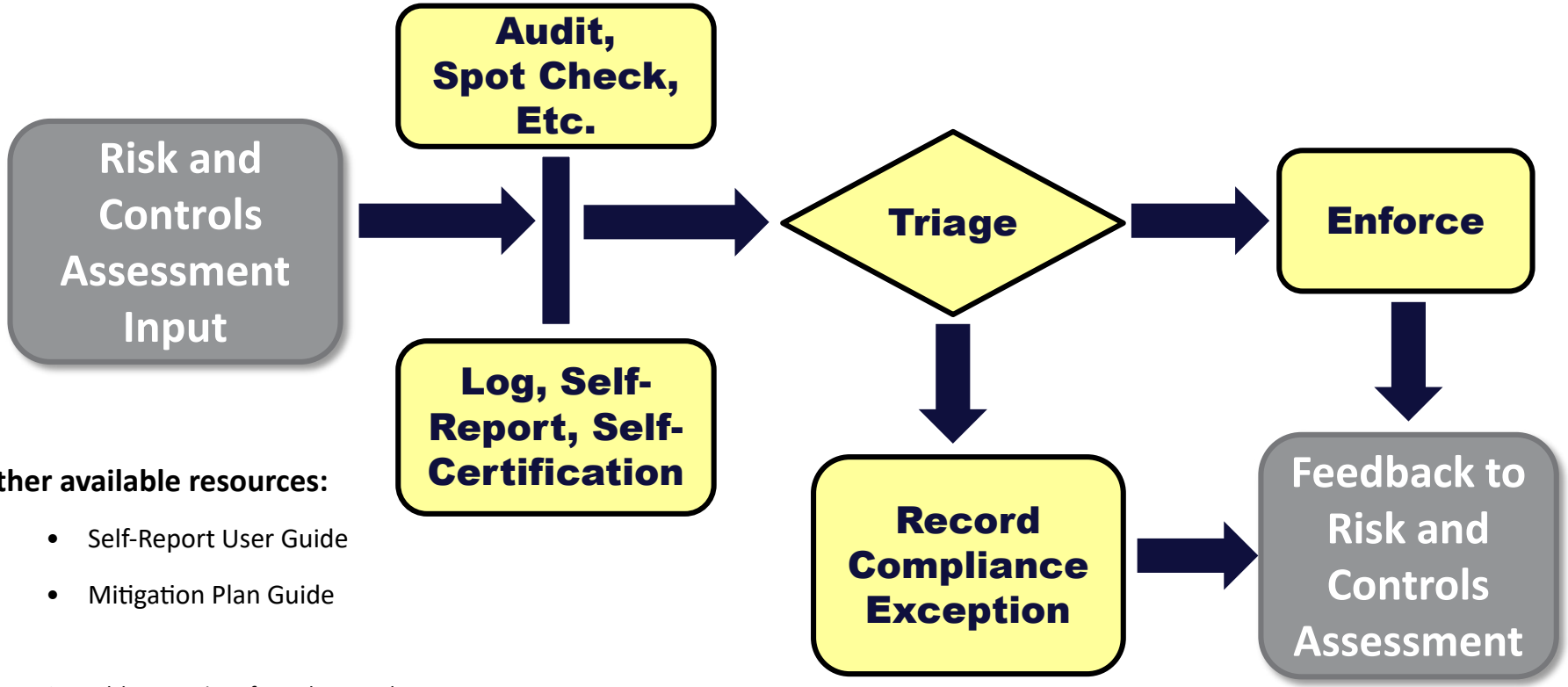
Noncompliance information is used as an input to other processes.

When developing risk elements, NERC annually identifies and prioritizes risks to the reliability of the BPS, taking into account factors such as compliance findings, event analysis experiences, and data analysis. In addition, Regional Entities may consider factors such as noncompliance information when conducting an Inherent Risk Assessment of a registered entity. The ERO Enterprise also uses noncompliance information as part of a feedback loop to the standards development process. This allows enhancement of Reliability Standards through appropriate information flows from compliance monitoring and enforcement to the standards drafting process and other NERC programs. NERC regularly provides analysis and lessons learned from noncompliance information to the public.[5]

[2] The NERC Rules of Procedure are available at http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx
[3] Posted Compliance Exceptions, FFTs, Spreadsheet Notices of Penalty, and Full Notices of Penalty are available at http://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx
[4] Quarterly enforcement program information is available at http://www.nerc.com/gov/bot/BOTCC/Pages/ComplianceCommittee(BOTCC).aspx
[5] For example, NERC posts quarterly compliance reports at http://www.nerc.com/gov/bot/BOTCC/Pages/ComplianceCommittee(BOTCC).aspx

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Enforcement Process Flow



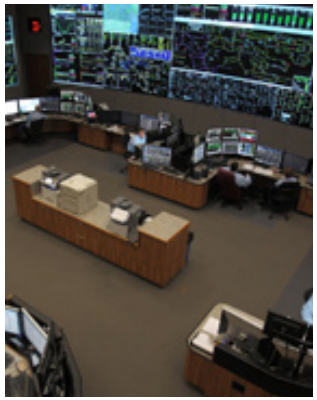
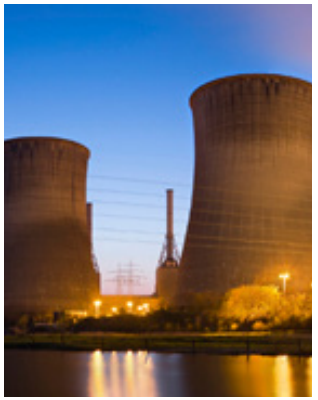
Other available resources:

- Self-Report User Guide
- Mitigation Plan Guide

Spreadsheet Notice of Penalty Template
Find, Fix, Track and Report (FFT) and Compliance Exception Template

ERO ENTERPRISE

Enforcement Competency Guide

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

VERSION 4 | 2018

ENFORCEMENT COMPETENCY GUIDE | TABLE OF CONTENTS

PREFACE

Electric Reliability Organization (ERO) Enterprise enforcement staff is responsible for resolving noncompliance with North American Electric Reliability Corporation (NERC) Reliability Standards in a fair, accurate, reasonable, and consistent manner. To accomplish this, enforcement staff possess a number of methods for resolving noncompliance issues, including streamlined enforcement processes, monetary sanctions, non-monetary sanctions, and remedial action directives. Enforcement staff will use one or more of these enforcement tools depending upon the particular facts and circumstances, as well as the degree of risk to the reliability of the bulk power system (BPS) posed by an issue. In all circumstances, enforcement staff will ensure that noncompliance is properly mitigated to address the reliability risk and prevent future recurrence.

To accomplish these tasks in a timely, efficient, and fair manner, the ERO Enterprise must have grounded principles and approaches whereby it acquires, develops, and retains personnel to perform enforcement activities. To this end, the Enforcement Capabilities and Competency Guide (Guide) is designed to provide a practical, hands-on resource for NERC and Regional Entity staff members and managers in identifying the combination of skills, attributes, and behaviors *(i.e., competencies)* that are necessary for the successful performance of various enforcement roles. Such competencies are important for all staff, regardless of occupation, function, or level.

The purpose of the Guide is not to definitively prescribe job descriptions. Rather, it identifies common levels of education and experience necessary to execute high-quality enforcement, risk assessment, and mitigation activities. It also provides information regarding the foundational and enforcement competencies for the functional roles that comprise the enforcement process across the ERO Enterprise. As such, the Guide provides expectations that Regional Entities should consider when developing their specific enforcement job descriptions. Because basic capabilities and competencies are necessary to produce a consistent product and approach across the ERO Enterprise, NERC may also use this Guide in its oversight of Regional Entity enforcement activities.

AUTHORITATIVE GUIDANCE

The following is a sampling of sources which informed the development of this Guide.

Rules of Procedure – Section 400 – Compliance Enforcement:

Section 401.4 – Role of Regional Entities in the Compliance Monitoring and Enforcement Program — Each Regional Entity that has been delegated authority through a delegation agreement or other legal instrument approved by the Applicable Governmental Authority shall, in accordance with the terms of the approved delegation agreement, administer a Regional Entity Compliance Monitoring and Enforcement program to meet the NERC Compliance Monitoring and Enforcement Program goals and the requirements in this Section.

Section 403.5 – Regional Entity Compliance Staff – Each Regional Entity shall have sufficient resources to meet delegated compliance monitoring and enforcement responsibilities, including the necessary professional staff to manage and implement the Regional Entity Compliance Monitoring and Enforcement Program.

Section 403.6 – Regional Entity Compliance Staff Independence – The Regional Entity Compliance Staff shall be capable of and required to make all determinations of compliance and noncompliance and determine Penalties, sanctions, and Remedial Action Directives and to review and accept Mitigation Plans and other Mitigating Activities.

Compliance Monitoring and Enforcement Program – Appendix 4C:

Section 5.0 – Enforcement Actions – "The Compliance Enforcement Authority shall determine (i) whether there have been violations of Reliability Standards by registered entities within the Compliance Enforcement Authority's Area of Responsibility, and (ii) the appropriate Mitigating Activities, and Penalties and sanctions as prescribed in the NERC Sanction Guidelines *(Appendix 4B to the NERC Rules of Procedure)*, as necessary. NERC will work to achieve consistency in the application of the Sanction Guidelines by Regional Entities by direct oversight and review of Penalties and sanctions, and each Regional Entity shall provide to NERC such information as is requested by NERC concerning any Penalty, sanction, or Mitigating Activities imposed by the Regional Entity."

PROFESSIONAL STANDARDS, ETHICAL PRINCIPLES, AND RULES OF CONDUCT

The ERO Enterprise enforcement staff evaluate compliance with NERC Reliability Standards by applying appropriate technical and professional judgment, regulatory and legal expertise, and experience in the NERC and FERC regulatory environment. Enforcement staff must also effectively communicate to affected registered entities the status of enforcement actions and the basis for a particular finding, risk assessment, disposition method, and associated sanction (if any). It is the responsibility of enforcement staff to adhere to a level of standards and principles to fulfill their responsibilities in an effective and efficient manner and support fair, accurate, reasonable, and consistent enforcement dispositions.

Enforcement staff performing CMEP work are expected to understand and demonstrate the following fundamental principles:

Integrity

Enforcement staff integrity is central to the sound exercise of professional judgment. Integrity is the quality of being honest and having strong moral principles. For ERO Enterprise enforcement staff, integrity is evidenced by the way an enforcement staff member performs their work, maintains an objective attitude, supports assessments and dispositions with factual evidence, and remains free from bias.

Objectivity[1]

Enforcement staff must be free from conflicts of interest, in both fact and appearance, which affect impartiality and independence related to the entity or enforcement process, report, and/or sanction. Objectivity must be maintained in the way enforcement staff gather, evaluate, and communicate information, including enforcement dispositions, reports, Penalties, and sanctions.

Confidentiality[2]

Enforcement staff shall keep in confidence and not copy, disclose, or distribute any Confidential Information or any part thereof without the permission of the registered entity, except as otherwise legally required.

Competency

Enforcement staff must possess the professional competence to complete their work. Competence is a function of an enforcement staff member's knowledge, skills, education, and experiences. Enforcement staff are expected to maintain and grow their professional competence through continuing education, training, and professional development.

Professional Behavior

Enforcement staff members perform their work with honesty, diligence, integrity, and responsibility while avoiding conduct that may discredit the work of the ERO Enterprise. Professional behavior requires enforcement staff members to perform their duties in accordance with all applicable technical and professional standards.

[1] NERC Rules of Procedure, Section 403.6.2
[2] NERC Rules of Procedure, Sections 403.6.4 & 1500

CEA ROLE EXPECTATIONS

Role Descriptions and Expectations[3]

Risk Assessment and Mitigation Analyst[4]

Role

The **Risk Assessment and Mitigation Analyst** evaluates the facts and circumstances surrounding potential noncompliance to determine the risk posed to BPS reliability. Risk Assessment and Mitigation Analysts work with registered entities to obtain the information necessary to determine the root cause of a particular issue and develop mitigation activities that address the reliability risk posed by the particular noncompliance and prevent future recurrence of the issue.

Risk Assessment and Mitigation Analyst Position Expectations	
Task	**Activity**
Risk Assessment and Mitigation, and Related Activities	Evaluates the facts and circumstances surrounding potential noncompliance to determine risk presented to BPS reliability.
	Works with registered entities to obtain necessary information to support risk analysis and develop mitigation plans.
	Determines the acceptable mitigation activities and/or plans associated with noncompliance instances to ensure that mitigation activities address the risk to the BPS posed by a potential noncompliance and prevent its recurrence.
	Reviews and confirms mitigation activities or plans are acceptable.
	Tracks and verifies completion of mitigation plans.
	Coordinates and ensures records are properly recorded, tracked, and maintained for risk assessments and mitigation activities.
	Provides technical expertise regarding risk assessment and mitigation for the processing of contested violations.
	Reviews postings of NERC standards, policies, and related material for impact on the risk assessment and mitigation process.
	Develops and produces written materials that support risk assessments and the mitigation activity approval process.
	Exercises sound, independent judgment regarding risk assessments and mitigation activity reviews.
General	Develops reports and presentations on risk assessment and related mitigation activities for registered entities and Regional Entity staff.
	Mentors peers on risk assessment techniques as well as operational and technical knowledge.
	Works with computerized information systems to extract and analyze information.
	Achieves goals within established time and resource constraints.

[3] Each regional entity is responsible for further defining role expectations that may describe additional duties and functions. Certain roles and responsibilities may also be combined into a single position or split among multiple positions depending upon the regional entity's internal enforcement staff structure

[4] Risk Assessment and Mitigation Analysts engage in a number of functions and roles as part of the ERO Enterprise's Compliance Monitoring and Enforcement Program. The description of the Risk Assessment and Mitigation Analyst role in this guide only describes the enforcement-specific aspects of the Risk Assessment and Mitigation Analyst position, and not the entirety of the skills, competencies, and responsibilities such a position may have within each regional entity

CEA ROLE EXPECTATIONS

Role Descriptions and Expectations[3] (Cont.)...

Risk Assessment and Mitigation Manager[5]

Role

The **Risk Assessment and Mitigation Manager** is responsible for directing and managing multiple risk assessment activities as part of the overall enforcement process. The Risk Assessment and Mitigation Manager oversees the evaluation of the risk associated with noncompliance, including ensuring that risk assessments are developed in a consistent and fair manner. The Risk Assessment and Mitigation Manager also oversees the development of appropriate mitigation activities to address the reliability risk posed by a particular issue and prevent its recurrence. The Risk Assessment and Mitigation Manager manages the continued monitoring of active Mitigation Plans and verification that appropriate mitigation activities are completed.

Risk Assessment and Mitigation Manager Position Expectations	
Task	**Activity**
Risk Assessment and Mitigation Manager, and Related Activities	Reviews assessments of the risk posed to the BPS by potential noncompliance to ensure risk assessments are being performed in a fair, consistent, accurate, and effective manner.
	Reviews determinations of acceptable mitigation activities and/or plans to ensure that mitigation activities address the risk to the BPS posed by a potential noncompliance and prevent its recurrence.
	Manages overall caseload of risk assessment issues and mitigation activities.
	Oversees procedures for the continued monitoring of active mitigation plans and closure of completed mitigation plans to ensure noncompliance is corrected in a timely and effective manner.
	Meets with NERC staff regarding risk assessment activities and oversees preparation of materials for NERC/FERC oversight of the risk assessment process.
	Reviews NERC Reliability Standards, provides feedback to the NERC standards team regarding risks to the BPS that are not addressed in the standards, and offers input in the standards development process.
	Prioritizes the processing of issues and assigns risk assessments and mitigation plan reviews appropriately.
	Ensures the comprehensive tracking of process steps, evidence, reports, and activities related to risk assessments and mitigation activities.
	Prepares reports to document risk assessment and mitigation activities for the Regional Entity Board of Directors, NERC, and/or FERC.
	Meets with registered entities to provide individual feedback on risk, controls, and compliance.
	Develops presentations on risk assessment and related mitigation activities for registered entities and Regional Entity staff.
	Exercises sound, independent judgment regarding the review and oversight of risk assessments and mitigation activity.

[5] Risk Assessment and Mitigation Managers engage in a number of functions and roles as part of the ERO Enterprise's Compliance Monitoring and Enforcement Program. The description of the Risk Assessment and Mitigation Manager role in this guide only describes the enforcement-specific aspects of the Risk Assessment and Mitigation Manager position, and not the entirety of the skills, competencies, and responsibilities such a position may have within each regional entity

CEA ROLE EXPECTATIONS

Role Descriptions and Expectations[3] (Cont.)...

Risk Assessment and Mitigation Manager[5] (Cont.)...

Risk Assessment and Mitigation Manager Position Expectations (Cont.)...	
Task	**Activity**
General	Ensures annual staffing needs are met, including supporting the hiring of new Risk Assessment and Mitigation staff.
	Assists with the development of budgets.
	Establishes accurate and well-communicated procedures.
	Mentors staff and peers on risk assessment techniques as well as operational and technical knowledge.
	Works with computerized information systems to extract and analyze information.
	Achieves goals within established time and resource constraints.

CEA ROLE EXPECTATIONS

Role Descriptions and Expectations[3] (Cont.)...

Data Coordinator/Program Administrator/Paralegal

Role

Data Coordinators, Program Administrators, and/or Paralegals are responsible for providing support for enforcement activities, which may include a variety of administrative support activities, as well as coordinating with NERC legal and enforcement staff.

Data Coordinator/Program Administrator/Paralegal Position Expectations	
Task	**Activity**
Enforcement Process and Related Activities	Coordinates and communicates updates to NERC pertaining to status of enforcement activities.
	Assists in reviewing, facilitating, and tracking completion of mitigation activities and/or plans.
	Coordinates with enforcement staff to ensure that noncompliance is appropriately recorded and tracked.
	Assists in the preparation of enforcement disposition, risk assessment, and mitigation plan verification documentation.
	Assists with maintaining the confidentiality of registered entity information, including the redaction of CIP information from the monthly spreadsheets provided to NERC for posting.
	Updates and maintains databases of information relating to compliance and enforcement activities.
	Tracks deadlines and requests follow-up materials from registered entities and Regional Entity staff as directed by management.
	Ensures that the complete and final record is submitted to NERC for review.
	Assists with compiling evidence or other materials in response to oversight requests from NERC and/or FERC.
	Supports development of presentations and other outreach materials.
	Maintains process service lists, entity-contact lists, and other pertinent information for communicating with registered entities.
General	Assists with software enhancement testing as needed.
	Assists with updating and creating templates as needed.
	Provides technical support regarding word processing, document management, or other software as necessary for enforcement staff.
	Achieves goals within established time and resource constraints.

CEA ROLE EXPECTATIONS

Role Descriptions and Expectations[3] (Cont.)...

Enforcement Analyst/Enforcement Attorney

Role

The **Enforcement Analyst/Enforcement Attorney** is responsible for developing the evidentiary record and independently assessing the facts and circumstances surrounding the potential noncompliance with NERC Reliability Standards. The Enforcement Analyst/Enforcement Attorney prepares clear and concise analyses of noncompliance to support proposed disposition methods. The Enforcement Analyst/Enforcement Attorney also conducts research on applicable NERC precedents and standards to ensure the fair, reasonable, and consistent disposition of enforcement matters. The Enforcement Analyst/Enforcement Attorney applies the NERC Reliability Standards to the facts and circumstances of noncompliance to assist with the creation of compliance enforcement positions and outreach.

Enforcement Analyst/Enforcement Attorney Position Expectations	
Task	**Activity**
Enforcement Process and Related Activities	Reviews and assesses potential noncompliance in accordance with the NERC Rules of Procedure and related guidance.
	Conducts research and drafts analysis regarding applicable NERC precedents and Reliability Standards to ensure appropriate and consistent dispositions of noncompliance instances.
	Conducts discovery regarding noncompliance issues and ensures development of a complete evidentiary record regarding all noncompliance.
	Interfaces and effectively communicates with registered entity compliance and legal contacts regarding the status of open enforcement actions.
	Ensures all enforcement actions adhere to and respect all due process protections throughout the enforcement process
	Develops conclusions, analysis, and legal assessment of relevant NERC Reliability Standards and precedent to support management in establishing and articulating compliance enforcement positions.
	Drafts disposition documents pertaining to the enforcement of NERC Reliability Standards.
	Drafts violation notices to registered entities concerning assessments of noncompliance.
	Develops proposed penalty amounts, including inputs to the NERC penalty tool.
	Prepares drafts of settlement agreements to support enforcement management.
	Provides legal and/or technical expertise in support of the resolution of contested violations.
	Reviews NERC filings and guidance materials, as well as FERC orders, and provides guidance to enforcement staff on technical and legal issues as appropriate.
	Assists with the drafting, compilation, and submission of any required compliance filings or oversight materials to NERC or FERC.
	Exercises sound, independent judgment regarding the processing of noncompliance.
General	Develops reports and presentations on the enforcement process for registered entities and Regional Entity staff.
	Ensures all enforcement actions adhere to and respect all due process protections throughout the enforcement process
	Works with computerized information systems to extract and analyze information.
	Achieves goals within established time and resource constraints.

CEA ROLE EXPECTATIONS

Role Descriptions and Expectations[3] (Cont.)...

Enforcement Manager

Role

The **Enforcement Manager** oversees the analysis and final disposition of potential noncompliance with NERC Reliability Standards. The Enforcement Manager is responsible for ensuring that the enforcement team understands and follows ERO Enterprise enforcement guidance and the NERC Rules of Procedure. The Enforcement Manager also manages and oversees enforcement processes and records, including application of the NERC Sanction Guidelines. The Enforcement Manager directs and reviews enforcement staff's efforts related to planning and executing all facets of the enforcement process, including development of the evidentiary record, analysis, and proposed disposition method. The Enforcement Manager reviews all enforcement records for sufficiency of evidence and consistency with NERC precedent, as well as ensures that the final and complete record is submitted to NERC for review.

Enforcement Manager Position Expectations	
Task	**Activity**
Enforcement Process and Related Activities	Manages processes for the review and assessment of potential noncompliance in accordance with the NERC Rules of Procedure and related guidance.
	Reviews disposition documents to ensure that enforcement matters are resolved in a fair, consistent, accurate, and effective manner.
	Reviews the evidentiary record to ensure there is sufficient evidence to support a proposed disposition and a complete and final record is submitted to NERC.
	Manages overall caseload of noncompliance.
	Reviews and approves all violation notices and related correspondence to registered entities.
	Effectively and persuasively communicates with NERC Staff regarding enforcement activities and oversees preparation of materials for NERC/FERC oversight of the enforcement process.
	Reviews NERC Reliability Standards, provides feedback to the NERC standards team regarding applicability and enforceability of those Standards, and offers input in the standards development process.
	Prioritizes the processing of issues and assigns issues appropriately.
	Ensures the comprehensive tracking of process steps, evidence, reports, and activities related to risk assessments and mitigation activities.
	Prepares reports to document enforcement activities for the Regional Entity Board of Directors, NERC, and/or FERC.
	Effectively and persuasively communicates with registered entities to provide individual feedback on risk, controls, and compliance.
	Identifies and analyzes violations and enforcement trends.
	Develops presentations on enforcement activities for registered entities and Regional Entity staff.
	Reviews settlement documents and supporting materials.
	Oversees the development of penalty amounts, including inputs to the NERC penalty tool.
	Leads settlement negotiations.

CEA ROLE EXPECTATIONS

Role Descriptions and Expectations[3] (Cont.)...

Enforcement Manager (Cont.)...

Enforcement Manager Position Expectations (Cont.)...	
Task	**Activity**
Enforcement Process and Related Activities	Prepares materials for hearings, coordinates the development of expert testimony, provides expert testimony, and/or conducts cross-examination at hearing as appropriate.
	Identifies and analyzes possible enforcement ramifications regarding policy and strategic decisions and effectively communicates significant issues to appropriate staff.
	Exercises sound, independent judgment regarding the oversight and review of the processing of noncompliance.
General	Ensures annual staffing needs are met, including supporting the hiring of new enforcement staff.
	Assists with the development of budgets.
	Establishes accurate and well-communicated procedures.
	Mentors staff and peers on the enforcement process, as well as legal, operational, and/or technical knowledge.
	Works with computerized information systems to extract and analyze information.
	Achieves goals within established time and resource constraints.

Educational and Certification Requirements

In order to ensure the accurate, fair, consistent and efficient processing of noncompliance, the teams responsible for the enforcement process must collectively possess the knowledge, experience, education, and skills to execute such work. It is the ERO Enterprise's responsibility to identify the professional competence that is needed to perform the various enforcement activities described throughout this Guide.

The minimum expectations regarding the educational attainment and certifications for enforcement staff are provided in Table 1 *(on the next page)*. While the ERO does not specifically require levels of education or certification, Regional Entities should strongly consider blending educational backgrounds, legal degrees and related training, as well as technical certifications, with professional experience. Regional Entities should evaluate their organizations and determine the appropriate balance of education, experience, and background that their enforcement staff will need to perform their work.

CEA ROLE EXPECTATIONS

Table 1 – Education and Certification Requirements for Enforcement

Education and Certifications		Risk Assessment and Mitigation Analyst	Risk Assessment and Mitigation Manager	Data Coordinator/ Program Administrator/ Paralegal	Enforcement Analyst/ Enforcement Attorney	Enforcement Manager
Education	**Graduate Degree:** MBA, J.D., Engineering, Information Systems, or similar discipline	A	A	N/A	P (J.D. required for Attorneys)	P (J.D. required for Attorneys)
	Bachelor's Degree: *(Degree in Electrical Engineering, Accounting, Auditing, Information Systems, or similar technical discipline preferred)*	R	R	P	R	R
	Associate Degree: Electrical Engineering, System Operations, Information Systems, or similar technical discipline	A	A	A *(Associate Degree or Legal Certificate required for Paralegals)*	A	A
Professional Certification	Professional Engineer	P	P	N/A	A	A
	State Bar License(s)	N/A	N/A	N/A	P for Attorneys	P for Attorneys
	Auditor Certifications: Certified Internal Auditor, Certified Government Auditing Professional, Certified Quality Auditor, Certified Information Systems Auditor, or similar	A	A	N/A	A	N/A
	Operations and Planning: NERC System Operator Certification, or similar	A	A	N/A	A	A
	Cyber and Physical Security: Certified in Risk and Information Systems Control, Certified Information Systems Security Professional, Certified Information System Manager, Physical Security Professional, or similar	P	P	N/A	A	A
	Legal Specializations: Board certifications in administrative law, energy law, electricity law, or similar	N/A	N/A	N/A	A	A

Legend		
R	Required	The Certification and Education is required for the Role, or justification for suitable substitution is necessary
P	Preferred	The possession of the Certification and Education impacts the success within the Role
A	Alternate	Will be considered in connection with years of experience and knowledge
N/A		Does not apply for the selected Role

CEA ROLE EXPECTATIONS

Industry Knowledge and Experience

A combination of knowledge and experience allows enforcement staff to make professional judgments in an educated manner. Practical experiences are necessary for enforcement staff to execute the technical aspects of their roles. Blending technical and/or legal knowledge and experience is necessary for the ERO Enterprise to conduct enforcement activities in a consistent, fair, efficient, and reasonable manner.

The types of practical and industry-focused experiences applicable to the enforcement processes are set forth in Table 2. The knowledge and experience provided in this table is not intended to be an exhaustive list. Further, enforcement staff members are not expected to be proficient in each area. Rather, Table 2 is intended to provide guidance regarding the types of knowledge and experience that support the various aspects of the enforcement process at each Regional Entity.

An individual's knowledge and experience are assessed relative to their demonstrated level of capability and competency. The Individual Core Competency and Professional Competency matrices should therefore be referenced accordingly.

CEA ROLE EXPECTATIONS

Table 2 – Knowledge and Experience for Enforcement						
Knowledge and Experience		Risk Assessment and Mitigation Analyst	Risk Assessment and Mitigation Manager	Data Coordinator/ Program Administrator/ Paralegal	Enforcement Analyst/ Enforcement Attorney	Enforcement Manager
Operational & Technical	General understanding of bulk power system (BPS) operations	R	R	P	R	R
	General understanding of cyber security issues	R	R	P	R	R
	Understanding of the FERC/NERC Regulatory Process	P	P	P	R	R
	Understanding of NERC Reliability Standards and applicable precedents	R	R	N/A	R	R
	Understanding the NERC Functional Model	R	R	N/A	R	R
	Ability to assess risk to the BPS as a result of noncompliance of Reliability Standards	R	R	N/A	P	P
	Ability to prioritize the resolution of higher risk noncompliance while balancing the need to dispose of lesser risk matters	P	R	N/A	P	R
	Ability to identify and analyze causes of noncompliance and evaluate appropriate mitigating actions	R	R	N/A	P	P
	Judgment to determine appropriate enforcement action, disposition track, and appropriate sanction, if any	P	P	N/A	R	R
	Ability to compile full records for enforcement dispositions	R	R	R	R	R
	Ability to assess internal compliance programs and cultures of compliance	R	R	N/A	R	R
	Ability to apply the RoP, including the CMEP, fairly and with regard to due process rights for registered entities	R	R	R	R	R
	Ability to understand and identify how to treat confidential information	R	R	R	R	R
	Strong writing skills, including ability to write clearly, and express complicated concepts in a concise manner	R	R	P	R	R

Legend		
R	Required	The Certification and Education is required for the Role, or justification for suitable substitution is necessary
P	Preferred	The possession of the Certification and Education impacts the success within the Role
A	Alternate	Will be considered in connection with years of experience and knowledge
N/A		Does not apply for the selected Role

INDIVIDUAL CORE COMPETENCY MATRIX

Core Competencies are the primary strengths enforcement staff use to perform assigned work. Individuals possess varying levels of competencies that allow the ERO Enterprise to pool the knowledge, as well as technical and legal capabilities, to produce high-quality work throughout the various stages of the enforcement process.

CEA Staff Enforcement and Mitigation Roles Individual Core Competency Matrix

Family	Competency	Attribute	Functional Roles				
			Risk Assessment and Mitigation Analyst	Risk Assessment and Mitigation Manager	Data Coordinator/ Program Administrator/ Paralegal	Enforcement Analyst/Enforcement Attorney	Enforcement Manager
Foundational Competencies	Interpersonal	Conflict Management	○	◐	○	◐	●
		Ethics and Values	●	●	●	●	●
		Teamwork	◐	●	◐	◐	●
	Communication	Business, Legal, and Technical Writing	◐	●	◐	●	●
		Interviewing and Conversations	◐	◐	○	◐	◐
		Presentation	○	◐	○	◐	◐
		Listening	◐	◐	◐	◐	◐
	Functional, Technical, and Industry Knowledge	Time Management	◐	◐	◐	◐	◐
		Technology	◐	◐	●	◐	◐
		Application of Reliability Standards	◐	●	○	●	●
		Bulk Power System Fundamentals	●	●	◐	◐	◐
		Cyber Security	●	●	○	◐	◐
	Management	Directing Others	◐	●	◐	◐	●
		Organization	◐	●	●	◐	●
		Leadership	◐	●	◐	◐	●
		Team building	○	◐	○	○	◐

Symbol Key

Icon	Level	Description
○	Basic to Intermediate	Sufficient to broad understanding of the competency, demonstrating intermediate required skills and proactive execution
◐	Intermediate to Advance	Extensive understanding of the competency, demonstrating advanced required skills, proactive execution advanced leadership by example
●	Advanced to Expert	Complete understanding of the competency, demonstrating expert required skills, proactive execution, and leadership by example and by fostering the vision and environment

INDIVIDUAL CORE COMPETENCY MATRIX

CEA Staff Enforcement and Mitigation Roles Individual Core Competency Matrix (Cont.)...

Family	Competency	Attribute	Functional Roles				
			Risk Assessment and Mitigation Analyst	Risk Assessment and Mitigation Manager	Data Coordinator/ Program Administrator/ Paralegal	Enforcement Analyst/Enforcement Attorney	Enforcement Manager
Enforcement Competencies	Enforcement Fundamentals	Risk Assessment	●	●	○	◐	◐
		Root Cause Assessment	◐	●	○	◐	◐
		Mitigation Review and Development	●	●	○	◐	◐
		Negotiation	○	◐	○	●	●
		Penalty Assessment	○	○	●	●	●
		Documentation Development and Management	●	●	●	●	●
	Legal and Regulatory Knowledge	General Enforcement Process	◐	●	◐	●	●
		Processing of Noncompliance	◐	●	◐	●	●
		FERC Regulations, Rules, and Governance	◐	◐	○	●	●
		NERC Functional Model	●	●	○	◐	◐
	Enforcement Oversight	Process Review	○	◐	◐	◐	◐
		Quality Assurance	◐	●	●	◐	●
		Reporting	◐	◐	●	◐	◐

Symbol Key

Icon	Level	Description
○	Basic to Intermediate	Sufficient to broad understanding of the competency, demonstrating intermediate required skills and proactive execution
◐	Intermediate to Advance	Extensive understanding of the competency, demonstrating advanced required skills, proactive execution advanced leadership by example
●	Advanced to Expert	Complete understanding of the competency, demonstrating expert required skills, proactive execution, and leadership by example and by fostering the vision and environment

COMPETENCY DEFINITIONS

Competencies are the behaviors that encompass the knowledge, attitudes, motives, and skills that distinguish excellent performance. Individual and organizational success rely on a set of competencies that:

- Establish fair, uniform, and consistent criteria for decision making;
- Establish a common language for defining success across the ERO Enterprise; and
- Reinforce the ERO Enterprise unique culture.

The core set of competencies identified in the preceding tables are defined below.

Foundational Competencies

Interpersonal: Life skills used every day to interact with other people both individually and in groups.

Conflict Management – Steps up to conflicts, seeing them as opportunities; reads situations quickly; good at focused listening; can hammer out tough agreements and settle disputes equitably; can find common ground and promote cooperation with minimal disruption.

Ethics and Values – Adheres to an appropriate and effective set of core values and beliefs during both smooth and difficult times; acts in line with those values; rewards the right values and disapproves of others. Understands the requirements outlined in GAGAS and IIA-IPPF.

Teamwork – Quickly finds common ground and solves problems for the good of all; represents his/her own interests yet is fair to teams; solves problems with peers with minimal disruption; is seen as a team player and is cooperative; easily gains trust and support of peers; encourages collaboration; can be candid with peers.

Communications: Methods used to convey and receive information to achieve a desired effect.

Business, Legal, and Technical Writing – Able to write clearly and succinctly in a variety of communication settings and styles; can analyze issues and apply relevant precedent as necessary to construct a persuasive argument and/or justification for a particular action; can draft succinct and clear questions or requests for information to registered entities to obtain information necessary to evaluate noncompliance.

COMPETENCY DEFINITIONS

Foundational Competencies (Cont.)...

Interviewing and Conversations – Conducts discussions in a manner that puts people at ease and builds constructive dialogue; appropriately plans for conversations through preparation and breadth of questions; maintains an objective attitude during discussions that are intended to obtain facts in support of fair, reasonable, and consistent outcomes.

Presentation Skills – Effective in a variety of formal and informal presentation settings: one-on-one, small and large groups, or with peers, direct reports, and supervisors; is effective both inside and outside the organization, on both current data and controversial topics; commands attention and can manage group dynamics; can change tactics midstream when necessary.

Listening Skills – Practices attentive and active listening; has patience to hear people out; can accurately restate the opinions of others even when in disagreement.

Functional, Technical, and Industry Knowledge: Subject matter expertise and background, as well as technical knowledge and skills to perform their designated role.

Time Management – Uses time effectively and efficiently; values other Regional Entity staff and registered entity's time; performs preliminary work to focus questions and streamline process; concentrates efforts on priorities; can attend to a broader range of activities.

Technology – Able to select and apply contemporary forms of technology to solve problems or compile information; has knowledge of and uses MS Office products; has experience using technology to analyze information or data; has experience using technology as venue for information sharing; able to determine which technologies apply to the task and understand the limitations of those technologies.

Application of Reliability Standards – Maintains awareness of NERC continent-wide standards, NERC standards under development, and related projects and activities; familiar with relevant NERC precedent, including approved mitigation and sanctions *(if any)*.

Bulk Power System Fundamentals – Understands the fundamentals and structure of the bulk power system, including interconnected power system operations; general knowledge and understanding of transmission system operation, substation and system protection; general knowledge and understanding of generation and power plant characteristics; general knowledge of the reliability coordination process; general knowledge and understanding of functional relationships and responsibilities for grid operation, physical security approaches and systems, control center operations, real-time studies, design, planning, and operations.

COMPETENCY DEFINITIONS

Foundational Competencies (Cont.)...

Cyber Security – General knowledge and understanding of operating systems, databases, network architecture, applications, software patching, and firewalls; general knowledge and understanding of physical security approaches and systems, as well as system access security.

Management: Management skills necessary to lead organizational strategy, drive activities, and develop enforcement staff.

Directing Others – Establishes clear directions; sets stretching objectives; distributes the workload appropriately; lays out work in a well-planned and organized manner; maintains two-way dialogue with others on work and results; brings out the best in people; is a clear communicator.

Organization – Marshals resources *(people, funding, material, and support)* to get things done; can orchestrate multiple activities at once to accomplish a goal; uses resources effectively and efficiently; arranges information and files in a useful manner.

Leadership – Leads people toward meeting the ERO Enterprise's vision, mission, and goals; provides an inclusive workplace that fosters the development of others; facilitates cooperation and teamwork; supports constructive resolutions to conflict.

Team Building – Blends people into teams when needed; creates strong morale and spirit in teams; shares wins and successes; fosters open dialogue; lets people finish and be responsible for their work; defines success in terms of the whole team; creates a feeling of belonging in the team.

Enforcement Competencies

Enforcement Fundamentals:

Risk assessment – Understands and is able to assess the risk posed by a noncompliance to the bulk power system; able to assess and identify the compensating factors present at the time of the noncompliance that mitigate or reduce the risk or potential for harm.

Root cause assessment – Able to determine the cause behind a noncompliance by understanding the complete facts and circumstances of the noncompliance; able to identify and determine factors that mitigate the noncompliance as well as prevent future recurrence of the issues in question.

COMPETENCY DEFINITIONS

Enforcement Competencies (Cont.)...

Mitigation Review and Development – Able to identify and determine factors that mitigate the noncompliance as well as prevent future recurrence of the issues in question; general knowledge and understanding of effective mitigation activities performed by other registered entities for particular issues and standards, and can apply those benchmarks to mitigation development.

Negotiation – Able to negotiate in all aspects associated with the enforcement cycle, including discovery, settlements, disposition, and penalties.

Penalty Assessment – Understands and able to use the NERC Sanction Guidelines to determine the appropriate penalty or sanction to be applied to a noncompliance; familiar with non-monetary sanctions; familiar with distinctions between necessary mitigation activities and "above and beyond" activities for which a registered entity may receive credit in the penalty calculation.

Documentation Development and Management – Able to draft concise descriptions of relevant facts and circumstances surrounding a noncompliance; can track document versions; can edit written materials and provide edits as appropriate; general knowledge and understanding of document and information management tools; general knowledge and understanding regarding the handling of confidential information and document security.

COMPETENCY DEFINITIONS

Enforcement Competencies (Cont.)...

Legal and Regulatory Knowledge:

General Enforcement Processes – Understands the role of various CEA staff in the enforcement processes; understands the role of various enforcement disposition methods as part of the risk-based enforcement paradigm; understands and applies the NERC Rules of Procedure to the enforcement process; applies NERC guidance as it relates to findings.

Processing of Noncompliance – Able to work with registered entities to obtain additional information pertaining to noncompliance and related mitigation; can document evidence and draft concise descriptions of relevant facts and circumstances surrounding noncompliance; able to draft notices and correspondence with registered entities and do so in a timely and efficient manner.

FERC Regulations, Rules, and Governance – Understands basic principles related to the ERO's legal authority to enforce Reliability Standards, the structure of the ERO, and duties delegated to the Regional Entities; understands basic administrative law concepts, including application of burdens of proof and production to the NERC/FERC regulatory environment.

NERC Functional Model – Demonstrates knowledge of the functions that must be performed to ensure reliability of the bulk power system; applies Functional Model as the foundation and framework of Reliability Standards.

Enforcement Oversight:

Process Review – Able to perform oversight of the enforcement processes using checklists and applying knowledge of enforcement fundamentals.

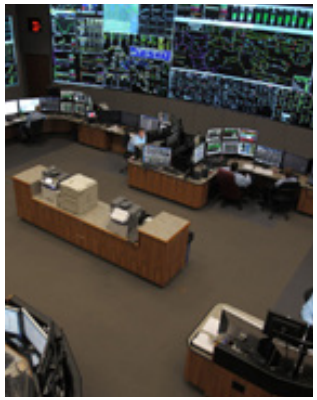
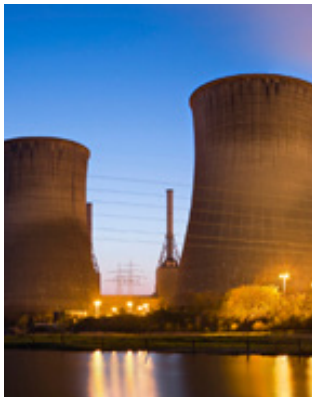
Quality Assurance – Able to determine and/or implement appropriate metrics to ensure the quality and timeliness of enforcement activities.

Reporting – Maintains detailed records regarding all aspects of the enforcement process to enable effective oversight and review; understands techniques to ensure the creation of a complete evidentiary and disposition record; understands and executes the Regional Entity's document retention policy.

ERO ENTERPRISE

Glossary

Glossary terms are based on the NERC Rules of Procedure, Generally Accepted Government Auditing Standards (GAGAS), the Institute of Internal Auditors International Professional Practices Framework (IIA-IPPF), and Public Company Accounting Oversight Board Standards.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

VERSION 4 | 2018

A

Action Owner: The person responsible for managing and completing the action item. The action item may be completed by another person but the Action Owner is responsible for the completion of the action item.

Action Reviewer: The person responsible for assuring the action is completed and correct. The person should be independent of the activity.

Analytical Procedures: Analytical procedures are used to assist in the nature, timing and extent of audit planning and testing by focusing on areas that may have a high degree of risk. They focus on the evaluation of data and can be used to identify unusual trends or events.

Annual CMEP Implementation Plan: The ERO CMEP Annual CMEP Implementation Plan is the annual plan for the ERO, both NERC and the Regional Entities, that identifies key CMEP activities and implementation.

Appropriate: Measure of the quality of evidence that encompasses the relevance, validity, and reliability of evidence used for addressing the audit objectives and supporting findings and conclusions.

Area of Concern (AOC): A situation that, if not addressed, could develop into future noncompliance. Ineffective or nonexistent preventive, corrective, or detective actions may contribute to an area of concern.

Audit Attendee: Person(s) attending an audit in a non-participatory role *(in whole or in part)*, which may include NERC or FERC observers, trainees, etc.

Audit Cycle: Auditing processes that auditors employ when conducting a compliance audit. The audit cycle includes the steps that an auditor will take to conduct the audit and assess a registered entity's compliance with Reliability Standards. The audit cycle includes Planning, Fieldwork, and Reporting.

Audit Management: Regional Management Group at each Regional Entity. May consist of an Audit Manager, Director of Compliance Audits, etc.

Audit Objective: Broad statements developed by auditors that define intended audit accomplishments.

Audit Period: Start and end dates the audit engagement encompasses. Refer to Section 3.1.4.2 for complete ERO audit period definition.

Audit Risk: Audit risk is the possibility that the auditors' findings, conclusions, recommendations, or assurance may be improper or incomplete, as a result of factors such as evidence that is not sufficient and/or appropriate, an inadequate audit process, or intentional omissions or misleading information due to misrepresentation or fraud.

Audit Universe: All Reliability Standards and Requirements applicable to the registered functions of the registered entity.

C

Compliance Auditor Role Expectations Guide: Guide describes the processes used to establish and determine the skill sets as well as associated initial and continuing training requirements for ERO Compliance Enforcement Authority staff.

GLOSSARY

Compliance Information Tracking System (CITS): A database used by some Regional Entities to store compliance related data.

Conclusions: Include Findings [PNC, No Finding (NF), Open Enforcement Action (OEA), and Not Applicable (NA)], Areas of Concern, and Recommendations.

Conflicts of Interest Form: Periodic forms, declarations, or acknowledgments to document a freedom of impairment or bias that could impact objectivity.

Confirmation: Testing approach that obtains a representation of information used to validate an existing function of a control or process.

Cryptographic Hash: An information security application used to assure the integrity of evidence files.

D

Deficiency (of evidence): The wrong type or format of evidence to allow a conclusion.

Deficient: Evidence lacks an essential quality or element or is inadequate in amount or degree to demonstrate compliance with a Reliability Standard.

Documentation Review: A testing approach for collecting and validating evidence that supports a policy, process, or procedure.

E

Engagement: Any compliance action performed to obtain reasonable assurance of a registered entity's compliance with Reliability Standards *(e.g., audits, spot checks, etc.)*.

Event Analysis Report (EAR): Addresses in detail the sequence of events as they occurred, the identified causal factors, and the appropriate corrective actions.

Evidence: All the information used by the Compliance Auditor in arriving at the conclusions during the audit.

Evidence Request: Evidence request, interchangeable with Requests for Information or data request, is a request made from the Regional Entity to the registered entity for specific information to support completion of the audit.

F

Facilities: A registered entity's buildings, plants, or structures used to support the BPS *(this term is not the same as Facility as defined NERC glossary)*.

Feedback Form: A NERC form a registered entity uses to provide comments on the Regional Entity's audit process and performance.

Final Approver: The person assigned to approve the work completed in the action item.

Finding: Results from audit activities.

Findings: Includes Potential Noncompliance (PNC), No Finding (NF), Open Enforcement Action (OEA), and Not Applicable (NA).

Functional Registration: Processes undertaken by NERC and Regional Entities to identify which registered entities are responsible for reliability functions within the Regional Entity's Region.

GLOSSARY

I

Inherent Risk: The risk that an activity would pose if no controls or other mitigating factors were in place *(the gross risk or risk before controls)*. A registered entity's inherent risk is a function of its various functional registrations and other relevant factors like its system design, configuration, interconnections, size, etc.

Inherent Risk Assessment (IRA): A review of potential risks posed by an individual registered entity to the reliability of the BPS.

Inquiry: A testing approach that consists of seeking information of knowledgeable persons inside or outside a registered entity. Inquiries are used to collect evidence and may range from formal evidence requests to informal oral inquiries.

Insufficient: Quantity and/or quality of supplied evidence is inadequate to determine compliance with a Reliability Standard.

K

Key Reliability Standard Spot Check (KRSSC): A NERC oversight project that is designed to enhance reliability through effective and rigorous compliance audits throughout North America.

L

Leadsheet: Document that serves as a summary or index of information. It cross-references to workpapers or to tick marks to link information.

M

Management Controls: Registered entity practices that provide a level of reasonable assurance that work is being completed properly with no violations of Reliability Standards, contributing to increased reliability of the Bulk Power System.

N

Network Diagram: A graphical depiction of nodes and connections in a computer or telecommunications network.

Not Applicable: A Compliance Enforcement Authority (CEA) determination that compliance monitoring was not required because:

- The Requirement did not apply to the Registered Entity based on the functions for which the entity is registered in the NERC Compliance Registry; or
- The requirement applies to the registered entity based on the functions for which the entity is registered, but the entity demonstrated it did not own or operate the Bulk Electric System (BES) Element or System or Cyber Asset that the Requirement references (e.g., the entity did not possess black start units, special protection systems (SPS), under-voltage load shedding (UVLS), etc.).

No Finding (NF): A determination that there is reasonable assurance that there is no instance of noncompliance with a Reliability Standard or Requirement.

O

Observation: A testing approach performed by the audit team that consists of looking at a process or procedure being performed by others as a method for collecting evidence.

GLOSSARY

Observer: As defined by CMEP, an observer is in addition to the audit team members. The following may participate as observers: (i) NERC Staff (which may include contractors to NERC); (ii) other members of the Regional Entity's Compliance Staff; (iii) with the permission of the Regional Entity, Compliance Staff members of other Regional Entities; and (iv) representatives of FERC and of other Applicable Governmental Authorities so long as the registered entity is subject to the Applicable Governmental Authority's reliability jurisdiction.

One-line Diagrams: Drawings of a registered entity's electrical system.

Open Enforcement Action (OEA): A potential noncompliance already identified and in the process of being mitigated. This may involve review of ongoing mitigation action(s) taken by the Registered Entity to correct or prevent recurrence of noncompliance for a Reliability Standard or Requirement.

P

Physical Examination: Testing approach that consists of a review, walkthrough, or an inspection of records, documents, or other tangible assets used as a method for collecting evidence.

Positive Observation: A conclusion reached during an audit that relates favorably with respect to the quality of the registered entity's processes, controls, or corporate culture of compliance.

Potential Noncompliance (PNC): A determination that there is a possible failure to comply with a Reliability Standard or Requirement.

Potential Noncompliance Worksheet: Documentation used to record the facts and circumstances of a Potential Noncompliance.

R

Reasonable Assurance: The degree of satisfaction the Compliance Auditor must have to support audit conclusions based on evidence gathered during the engagement.

Recommendation (REC): Suggested improvements in the compliance program, control-related processes, procedures, or tools to enhance the reliability, security, or resiliency of the BES. Opportunities for process improvements should be shared with the Registered Entity.

Reperformance: A testing approach that consists of an independent execution of procedures or controls that were originally performed by the registered entity to determine if the same result is achieved.

S

Sampling: Audit procedure to select less than 100 percent of the items being tested. Sampling allows the audit team to evaluate a subset of the items being tested when a review of all items would cause time or cost restraints. *(Note: Sampling Guide includes a Glossary for terms used during sampling).*

Subject Matter Expert (SME): Refers to the person responsible for compliance with a Reliability Standard or Requirement at a registered entity.

Substantive Testing: Detailed testing performed by the Compliance Auditor to gather evidence as to the completeness, validity and accuracy of evidence to assess the registered entity's compliance with a Reliability Standard or Requirement.

GLOSSARY

Sufficiency: Measure of the quantity and adequacy of evidence used to support the findings and conclusions related to the audit objectives. Auditors should determine whether enough evidence has been obtained to persuade a knowledgeable person that the findings are reasonable.

Summary Table: A section of the RSAW that compiles the detailed results of the testing for the Requirements within Reliability Standard.

T

Technical Feasibility Request (TFE): An exception from strict compliance with the terms of an applicable Requirement on grounds of technical feasibility or technical limitations in accordance with one or more of the criteria in Section 3.0 of ROP Appendix 4D.

Test/Testing: The process or approach for evaluating evidence from a registered entity.

Testing Approach: Specific procedures used by a Compliance Auditor to collect and test audit evidence. Testing approaches include: inquiry, observation, physical examination, Reperformance, and confirmation.

Test Plans: The testing approach and documents *(e.g., RSAW Compliance Assessment Approach specific to the Reliability Standard and Requirement)* used to conduct the audit to meet the audit objectives.

Tick Marks: Abbreviations and symbols used by Compliance Auditors to denote auditing actions performed.

W

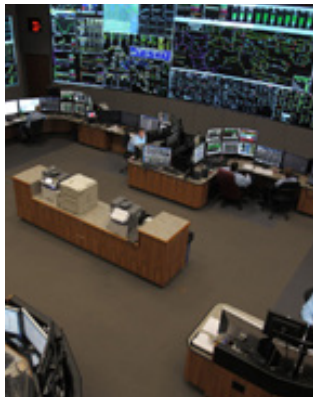
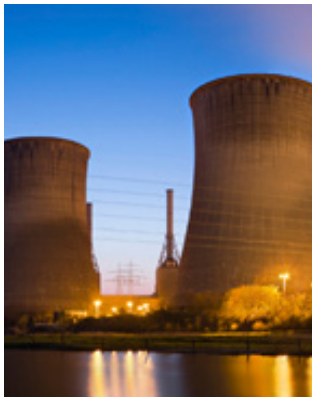
WebCDMS: A Compliance Data Management System (CDMS) used by some Regional Entities to store and maintain compliance data.

Workpapers: Audit documentation, retained by the auditor, of procedures applied, tests performed, information obtained or prepared, and pertinent conclusions of the engagement.

Glossary terms are based on the NERC Rules of Procedure, Generally Accepted Government Auditing Standards (GAGAS), the Institute of Internal Auditors International Professional Practices Framework (IIA-IPPF), and Public Company Accounting Oversight Board Standards.

ERO ENTERPRISE

CIP Version 5 Evidence Request

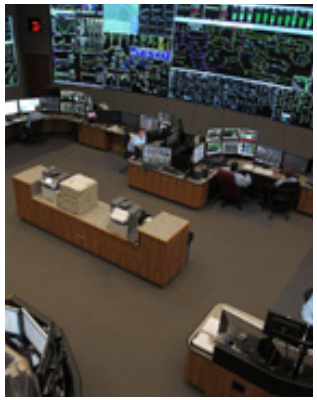
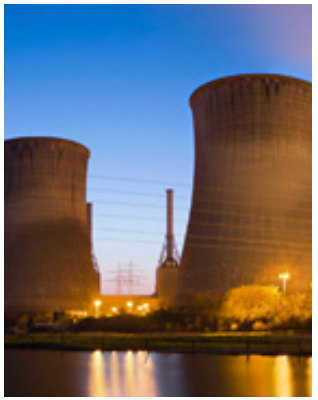
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

VERSION 4 | 2018

CIP Version 5 Evidence Request and User Guide.

ERO ENTERPRISE

Revision History Table

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

VERSION 4 | 2018

REVISION HISTORY TABLE

Update on Compliance Monitoring and Enforcement Manual: Description of Revisions

Version	Date	Revision Detail
Version 1.0	April 30, 2014	• Finalized grammar, charts, graphics and links. Final draft of version 1 posted to NERC's website.
Version 2.0	August 4, 2015	• Completed edits and corrections that have been compiled since the original Manual posting in April 2014. These edits and corrections were received from Regional Entity staff and the Manual Task Force (MTF). They are minor in nature and do not reflect significant changes in content. • Incorporated the Authoritative Guidance for CMEP Work document as a separate chapter in the Manual. This section also incorporates a new graphical layout. • Changed all references of the ERO Enterprise Compliance Auditor Manual to the ERO Enterprise Compliance Monitoring and Enforcement Manual. • Updated Foreword section of the manual with revised language. • Updated the Glossary to encompass the entire Compliance Monitoring and Enforcement Manual, rather than just the Auditor Handbook section of the Manual. • Apply applicable marked-up PDF edits to the overall Manual. • Consolidated the Manual, Compliance Auditor Introduction and the Introduction to Compliance Auditing into a single introduction in the Compliance Auditor Handbook and Checklist section of the Manual. • Incorporated the ECEMG approved Sampling Handbook as a separate chapter, and changed the name to Sampling Guide. • Incorporated the current version of the Compliance Auditor Capabilities and Compliance Monitoring Competency Guide. An updated version of this document is currently being developed by a vendor (QTS). • Updated the Table of Contents to reflect the most recent revisions. • Introduced new cover page and divider page layouts, including a more easily readable navigation (i.e. shortened titles). • Updated the Infographics Key page to reflect the revised naming conventions. • Incorporated photos on divider pages. • Added a cross reference section (Authoritative Guidance vs. GAGAS). • Completed 2015 Manual Task Force (MTF) edits. • Changed all instances of BES to BPS and changed the standard names from PER5, PRC5, FAC3, etc. to PER-005, PRC-005, FAC-003, etc. • Incorporated the Lead Sheet Template in the Sampling Guide section. • Revised the Revision History Table. • Finalized grammar, charts, graphics and links. • Approved by ERO EMG.

Update on Compliance Monitoring and Enforcement Manual: Description of Revisions

Version	Date	Revision Detail
Version 2.0 (Cont.)...	August 4, 2015 (Cont.)...	• Completed redline edits from MTF team and Craig Struck. • Posting of Manual.
Version 3.0	July 6, 2016	• Completed “Enforcement” section design samples. • Completed “Competency Guide” charts, graphics and infographics. • Completed redline edits from Craig Struck. • Added references to: ERO Enterprise Inherent Risk Assessment (IRA) Guide, ERO Enterprise Internal Control Evaluation (ICE) Guide and Coordinated Oversight of Multi-Region Registered Entities Program Development and Implementation in the 02-0108 section. • Added the newest Competency and Capability tables in the “Compliance Monitoring Competency Guide” section. • Changed all references of ”2015” to “2016”. • Changed all references of ”Version 2” to “Version 3”. • Added “Enforcement Competency Guide” after the “Competency Guide”. • Updated the Glossary section. • Added the “Enforcement Process” flow chart/graph. • Changed all references of ”Competency Guide” to “Compliance Monitoring Competency Guide” throughout the document. • Added “Enforcement” information to the Table of Contents. • Deleted the sentence “In support of the Compliance Auditing practices and the Reliability Assurance Initiative (RAI), version 1 of the Auditor Handbook (Handbook) has been completed” from the “Compliance Auditor Handbook and Checklist” section. • Added the “Enforcement Process” flow chart/graphic. • Added “Annual CMEP Implementation Plan” (under Audit Planning). • Changed all references of ”Reliability Assessment” to “Inherent Risk Assessment” throughout the document. • Added ERO Enterprise Inherent Risk Assessment Guide and ERO Enterprise Internal Control Evaluation Guide (under Guiding Documents). • Changed title to read “Entity Profile and Inherent Risk Assessment” in the 02-0108 section. • Changed bullet 2 to read “Perform Inherent Risk Assessment per the IRA Guide to include” in the 02-0108 section. • Deleted bullet “a” and renumber remaining items in the 02-0108 section.

REVISION HISTORY TABLE

Update on Compliance Monitoring and Enforcement Manual: Description of Revisions

Version	Date	Revision Detail
Version 3.0 (Cont.)...	July 6, 2016 (Cont.)...	• Inserted bullet "h" "If this is a Multi-Regional Registered Entities (MRRE) audit, the Lead Regional Entity (LRE) shall coordinate with the Affected Regional Entities (ARE) to develop the combined IRA per the referenced MRRE Guide" in the 02-0108 section. • In bullet "b", changed "recommended Reliability Standards and Requirements" to "NERC Annual Risk Elements and Regional Risk Elements" in the 02-0108 section. • Deleted bullet "c" in the 02-0108 section. • Inserted as bullet "g" "If registered entity elected to participate in ICE, review registered entity Internal Control Evaluation (ICE). See ICE Guide for details" in the 02-0108 section. • Inserted bullet "h" "If this is a Multi-Regional Registered Entities (MRRE) audit, the Lead Regional Entity (LRE) shall coordinate with the Affected Regional Entities (ARE) to develop the combined IRA per the referenced MRRE Guide" in the 02-0108 section. • Added back the missing introduction page to the "Compliance Auditor Handbook and Checklist" section. • Changed the "Enforcement Process" flow chart/graphic to the "Risk Based Compliance Monitoring" flow chart/graphic. • Updated the "Revision History Table". • Updated the Manual Table of Contents. • Apply applicable marked-up PDF edits to the overall Manual. • Completed redline edits from Patrick Moast. • Completed redline edits from Craig Struck. • Formatted the document. • NERC management review of the Manual. • Added the "Enforcement Competency Guide" after "Enforcement". • Changed "Compliance Auditor Handbook Checklist" to "Compliance Auditor Checklist" (for all instances throughout the Manual). • Added "Enforcement Competency Guide" after "Enforcement" in the TOC. • Added a period after checklist on page 30. • Changed "Auditor Checklist" to "Compliance Auditor Checklist" (for all instances throughout the Manual).

Update on Compliance Monitoring and Enforcement Manual: Description of Revisions

Version	Date	Revision Detail
Version 3.0 (Cont.)...	July 6, 2016 (Cont.)...	• Changed "Checklist" to "Compliance Auditor Checklist" (for all instances throughout the Manual). • Changed "Handbook and Checklist" to "Compliance Auditor Handbook and Checklist" (for all instances throughout the Manual). • Updated the Manual RBCM graphic. • Changed "Checklist Action Item" to "Action Item" (for all instances throughout the Manual). • Changed "Audit Checklist" to "Compliance Auditor Checklist" (for all instances throughout the Manual). • Changed "Annual Implementation Plan (IP)" to "Annual CMEP Implementation Plan" (for all instances throughout the Manual). • Changed date from "December 2013" to "June 2016". • Updated the Enforcement section write-up. • Updated the Enforcement Process Flow graphic. • Added an "Enforcement Comp Guide" coming soon page. • Updated glossary: Added "Annual CMEP Implementation Plan" definition to "A". • Updated "Version 3" text to "Version 4" text (for all instances). • Update all text to reference correct page #'s (including the Competency Guide section). • Updated new Enforcement write-up. • Updated new CMEP graphic. • Added the footer to all pages throughout the Manual. • Completed redline edits from MTF team and Craig Struck. • Made footer link to home page (all instances). • Updated RBCM graphic links. • Performed Spell Check. • Updated all of the Table of Content pages. • Formatted the document. • Finalized all of the links and interactivity throughout the document. • Finalized the "Revision History Table".

Update on Compliance Monitoring and Enforcement Manual: Description of Revisions

Version	Date	Revision Detail
Version 3.0 (Cont.)...	July 6, 2016 (Cont.)...	• Changed "Enforcement" to "Risk-Based Enforcement" and changed "Coming Fall 2016" to "Coming Soon" (for all instances). • Added the following email addresses (pmoast@wecc.biz, craig.struck@NERC.net) to the feedback link (page 4 of 232). • Deleted "Process Timing: XXX-XXX days prior to audit" (page 46 of 232). • Replaced "TBD" with "Timing of coordination with Enforcement regarding Possible Violations is specific to each Regional Entity's handoff processes" (page 123 of 232). • Changed the instances of "Sampling Handbook" to "Sampling Guide" (page 161 of 232). • (Sampling Process Flows) - Inserted the Sampling Guide link in place of "xxxxxx..." (page 178 of 232). http://www.nerc.com/pa/comp/Documents/Sampling_Handbook_Final_05292015.pdf • (Risk-Based Enforcement) - Changed "Enforcement" to "Risk-Based Enforcement" (page 212 of 232). • (Enforcement Competency Guide) - Changed "Coming Soon: Fall 2016" to "Coming Soon – Document Under Development" (page 219 of 232). • (Acknowledgements) – Deleted these pages (pages 226 - 227 of 232). • (Revision History Table) – Updated Version 1, Version 2 and Version 3 to correct dates and sections (pages 226 - 230 of 231). • Changed all references in the Manual to indicate the current version is Version 3 vs . Version 4. • Completed redline edits from MTF team and Craig Struck. • Added appendices to the back of the document.

REVISION HISTORY TABLE

Update on Compliance Monitoring and Enforcement Manual: Description of Revisions

Version	Date	Revision Detail
Version 4.0	July 28, 2017	• Updated the "Revision History Table" to "include "Version 4". • Updated the Manual's edition from "Version 3" to "Version 4". • Updated the Manual's edition from "2016" to "2017". • Completed redline edits from Craig Struck. • Page 34 - Deleted "Pre-Audit Planning". • Pages 35-39 - Deleted pages. • Pages 40-42 - Future revisons to come (TBD). • Pages 43-49 - Deleted pages. • Pages 51-53 - Deleted pages. • Pages 55-56 - Deleted pages. • Pages 58-60 - Deleted pages. • Page 61 - Renumbered "02-0404" to "02-0201". • Page 62 - Deleted page. • Page 63 - Renumbered "02-0406" to "02-0202" and change "Establish Audit Milestones" to "Establish Audit Milestones, Goals and Expectations". • Page 64 - Deleted page. • Page 65 - Renumbered "02-0408" to "02-0203". • Page 66 - Deleted page. • Page 68 - Renumbered "02-0501" to "02-0301" and change Action Item to "Confirm independence and address conflicts of interest for each Compliance Auditor, Consultant, and Third Party team member. • Page 69 - Deleted page. • Page 71 - Deleted page. • Pages 73-74 - Deleted pages. • Page 75 - Renumbered "02-0800" to "02-0400". • Page 77 - Renumbered "02-0802" to "02-0402". • Page 78 - Renumbered "02-0900" to "02-0500". • Page 79 - Renumbered "02-0901" to "02-0501".

REVISION HISTORY TABLE

Update on Compliance Monitoring and Enforcement Manual: Description of Revisions

Version	Date	Revision Detail
Version 4.0 (Cont.)...	July 29, 2017	• Page 80 - Renumbered “02-0902” to “02-0502”. • Page 81 - Renumbered “02-1000” to “02-0600”. • Page 82 - Renumbered “02-1001” to “02-0601” change Action Item to “Utilize NERC approved “ERO Sampling Guidelines and Criteria” to develop samples to test in scope requirements and submit samples to entity. • Page 83 - Deleted page. • Page 86 - Added the sentence “Determine whether additional documentation is required to satisfy audit objectives” to the Action Item. • Page 88 - Deleted page. • Page 89 - Renumbered “03-0201” to “03-0201”. • Page 90 - Renumbered “03-0203” to “03-0202” change Action Item to “Send subsequent requests when required”. • Page 92 - Changed Action Item to “Schedule and conduct a final planning meeting to discuss expectations, milestones, agenda, status, communication protocol, and additional preparatory activities”. • Page 93 - Deleted page. • Page 98 - Added new page (after page 97), make number “03-0502” and make Action Item say “Send subsequent requests when required”. • Page 99 - Changed Action Item to “Update Auditor workpapers based upon work performed by the Audit Team, including sample testing”. • Page 100(old)/101(new) - Deleted page. • Page 104(old)/105(new) - Deleted page. • Page 105(old)/106(new) - Renumbered “03-0802” to “03-0802”. • Page 108(old)/109(new) - Deleted page. • Pages 111-114(old)/112-115(new) - Deleted pages. • Page 116(old)/117(new) - Changed Action Item to “Prepare the Exit Briefing presentation, prepare the brief, review the exit brief, and meet with entity PCC and management to discuss the reults of the Audit inlcuding potential noncompliance areas of concern, and recommendations. • Pages 117-118(old)/118-119(new) - Deleted pages. • Page 122(old)/123(new) - Deleted page. • Page 126 - Added new page (after page 125), make number “04-0202” and make Action Item say “Provide Risk Assesment department any lessons learned/entity information obtained during the Audit that could result in an update to the entities IRA”.

Update on Compliance Monitoring and Enforcement Manual: Description of Revisions

Version	Date	Revision Detail
Version 4.0 (Cont.)...	July 29, 2017	• Page 126(old)/128(new) - Changed Action Item to "Compile ERO standard draft report describing the results of the testing along with any Possible Noncompliance, Areas of Concern, and Recommendations". • Page 127(old)/129(new) - Deleted page. • Page 128(old)/130(new) - Renumbered "04-0303" to "04-0302" and changed Action Item to "Perform independent* management review of the draft report, including verifying report content supported by sufficuent and appropriate evidence". • Page 137(old)/139(new) - Deleted page. • Page 138(old)/140(new) - Renumbered "04-0603" to "04-0602". • Page 139(old)/141(new) - Deleted page. • Page 140(old)/142(new) - Renumbered "04-0605" to "04-0603". • Pages 143-145(old)/145-147(new) - Deleted pages. • Pages 146(old)/148(new) - Future revisons to come (TBD). • Updated the Manual Table of Contents to match the current non-redline draft. • Updated the Revision History Table to match the current non-redline draft. • Updated the Risk-Based Enforcement Table of Contents to match the current non-redline draft. • Updated the CIP Version 5 Evidence Request Table of Contents to match the current non-redline draft.
	August 18, 2017	• Kick off call with the NERC team for the next draft.
	September 17, 2017	• Updated the "Revision History Table" to "include "Version 5". • Updated the Manual's edition from "Version 4" to "Version 5". • Recreated the color wheel to match the new Compliance Auditor Handbook Table of Contents (from 5 colors to 3 colors). • Updated all instances of the original color wheel to the new color wheel. • Updated the Compliance Auditor Checklist to match the new color wheel. • Updated all instances of the original square color swatches to match the new color wheel (bottom right). • Updated the Compliance Auditor Handbook Table of Contents. • Deleted all process flow diagrams. • Updated all Action Item Steps. • Removed "Preliminary Audit Determination" from the Glossary.

REVISION HISTORY TABLE

Update on Compliance Monitoring and Enforcement Manual: Description of Revisions

Version	Date	Revision Detail
Version 4.0 (Cont.)...	September 18, 2017	• Globally replaced "ERO Sampling Handbook" with "ERO Enterprise Sampling Guide. • Global search for "2016" to replace with "Current Version". • Updated the Glossary.
	September 19, 2017	• Deleted all references to the purple and yellow color wheel throughout the document (including pages). • Updated the Manual to include of the edits that were provided to me by the team. • Made note of all of the missing information in the document in red to provide to the NERC team. • Made note of all of the questions to ask the NERC team for the next draft. • Updated all footnotes to a smaller and consistent font size. • Updated Handbook and Checklist headings to the samething. • Used the first sentence of the Checklist Task sentence without bullets in the Action Items Step Process Flow Box. • Changed the format to "0N-0000" throughout the document. • Globally replaced the term "Preliminary Audit Determination" with "Audit Team Conclusions" throughout the Manual. • Globally replaced the term "Possible Violation" with "Potential Noncompliance" throughout the Manual. • Updated all footnotes to a smaller and consistent font size. • Globally added "Complete the Compliance Auditor Checklist Action Item" as the last item on the list of action item steps. • Emailed Craig Struck (cc'd Andrew Williamson and Dennis Glass) Draft 26 of the Manual.
	September 24, 2017	• Updated the Enforcement Competency Guide. • Updated the Revision History Table. • Formatted the document. • Update table page #'s within the documents (pages 140, 142 and 144 – formerly highlighted in red text) to "on the next page".
	October 1, 2017	• Completed the Enforcement Competency Guide. • Updated the Revision History Table. • Updated the Glossary. • Formatted the document. • Emailed Craig Struck (cc'd Andrew Williamson and Dennis Glass) Draft 27 of the Manual.

Update on Compliance Monitoring and Enforcement Manual: Description of Revisions

Version	Date	Revision Detail
Version 4.0 (Cont.)...	December 5, 2017	• Emailed Craig Struck (cc'd Andrew Williamson and Dennis Glass) Draft 28 of the Manual.
	December 9, 2017	• Changed "Compliance Monitoring" to "CMEP activities" on the Infographics Key page. • Deleted Footnote 1 and renumbered all Footnotes throughout the Manual to match the new order (Authoritative Guidance for CMEP Work). • Deleted Footnote 1 and renumbered all Footnotes throughout the Manual to match the new order (Risk-Based Enforcement). • Globally replaced the term "Non-Compliance(s)" to "Noncompliance(s)" without the hyphen throughout the Manual. • Updated various individual section of the Manual that was missing content (such as "Anticipated Start"). • Ensured "Non-Public" includes hyphen throughout the Manual.
	December 16, 2017	• Updated the color wheel to match the new information. • Updated the color swatches to match the new information. • Update the Infographics Key page to match the new information. • Added two infographics to the Infographics Key page (Task and Task/Action Item Highlights). • Updated the Compliance Auditor Handbook from 5 sections to 3 sections. • Updated the Compliance Auditor Handbook "Tasks #'s". • Changed "Manual and Compliance Auditor Handbook" to "Compliance Monitoring and Enforcement Manual and Auditor Handbook" on the Infographics Key page. • Changed "Compliance Auditor Handbook" to "Auditor Handbook" on the Infographics Key page.
	December 26, 2017	• Updated all of the Table of Content pages. • Matched the "Enforcement Competency Guide" section to the "Compliance Monitoring Competency Guide" section (including the charts). • Completed redline edits from Craig Struck (and team). • Added a tabular system to the Manual for easier naviagtion.

REVISION HISTORY TABLE

Update on Compliance Monitoring and Enforcement Manual: Description of Revisions

Version	Date	Revision Detail
Version 4.0 (Cont.)...	December 29, 2017	• Updated all interactivty. • Formatted the document. • Spell checked the document.
	December 30, 2017	• Linked the Glossary terms within the document. • Updated the Revision History Table. • Emailed Craig Struck (cc'd Andrew Williamson and Dennis Glass) Draft 29 of the Manual.
	January 26, 2018	• Changed "ERO Enterprise Guide for Internal Control Evaluation" to "ERO Enterprise Guide for Internal Controls" in the Audit Planning section of the Compliance Auditor Handbook section. • Updated the links in the "Risk Based Process Flow" section. • Updated the links in the "Enforcement Process Flow" section. • Updated the links in the "CIP Version 5 Evidence Request" and "User Guide" sections.
	January 27, 2018	• Updated the Glossary terms. • Put the Glossary terms in alphabetical order. • Globally replaced the term "Preliminary Audit Determinations" to "Audit Team Conclusions" throughout the Manual. • Globally replaced the term "Possible noncompliance" to "Potential Noncompliance" throughout the Manual. • Globally replaced the term "Compliance Auditor Handbook" to "Auditor Handbook" throughout the Manual. • Updated the email distribution list for Manual feedback. • Updated the links to the Yellow Book.
	January 28, 2018	• Made the "Area Overview" sections consistent throughout the Manual. • Changed "01-0101 | Audit Planning >> Audit Scoping >> ATL to Obtain the IRA and COP, and Develop the Audit Scope" to "01-0101 | Audit Planning >> Audit Scoping >> ATL to Obtain the IRA and COP, and Finalize the Audit Scope". • Added "Varies based on Regional processes" to all blank "Task Timing" sections. • Updated "Task Timing", "Process Timing", "Action Item Tips & Techniques", "Action Item Steps", "Key Documents to Complete", "Action Item References", and "Action Item" sections.

Update on Compliance Monitoring and Enforcement Manual: Description of Revisions

Version	Date	Revision Detail
Version 4.0 (Cont.)...	January 29, 2018	• Changed Revision History Table from "Version 5" to "Version 4" and throughout the Manual. • Re-formatted the document. • Updated the Revision History Table. • Updated the tabular system from "CA Handbook" to "Auditor Handbook" for consistency. • Emailed Craig Struck (cc'd Andrew Williamson and Dennis Glass) Draft 30 of the Manual.
	January 31, 2018	• Globally replaced the term "Compliance Auditor Checklist" to "Auditor Checklist" throughout the Manual. • Revised the Glossary Term Recommendation. • Re-updated all interactivty. • Re-spell checked the document. • Completed redline edits from MTF team and Craig Struck.
	February 01, 2018	• Re-linked the Glossary terms within the document. • Emailed Craig Struck (cc'd Andrew Williamson and Dennis Glass) Draft 31 of the Manual.
	February 07, 2018	• Emailed Craig Struck (cc'd Andrew Williamson and Dennis Glass) Draft 32 of the Manual.
	February 09, 2018	• Removed Action Item # "02-402: Perform review of the Audit Notification Packet (person other than the preparer)." • Changed "Prepare the deliver the Exit Briefing presentation" to "Prepare and deliver the Exit Briefing presentation" in Action Item 02-1101. • Emailed Craig Struck (cc'd Andrew Williamson and Dennis Glass) Draft 33 and Draft 34 of the Manual.

VERSION 4 | 2018