

RELIABILITY & SECURITY

Workshop—San Diego, CA

OCTOBER 31—NOVEMBER 1





Using the Work of Others

October 31, 2023

Lonnie Ratliff, Director of Compliance Assurance and Certification, NERC

Morgan King, Senior Technical Advisor, Cyber Security, WECC

Aldo Nevarez, Senior Auditor, Cyber Security Entity Monitoring, WECC

Tom Williams, Manager, Entity Monitoring, WECC

What Will You Learn and Why it Matters

- Explore the practice guide *Using the Work of Others* and learn:
 - What "others" means
 - What "work" qualifies
 - How the generally accepted audit practice of using the work of others applies to your audit
- Using the work of others can support findings at the current audit, avoid duplication of effort, and streamline the audit experience

Guidance

GAGAS Yellow Book

The Yellow Book refers to auditing standards of the U.S. Government Accountability Office, commonly referred to as “generally accepted government auditing standards” (GAGAS).

Sections 8.80-8.86 of the Yellow Book specifically cover using the work of others within the chapter covering fieldwork standards for performance audits.



United States Government Accountability Office
By the Comptroller General of the
United States

April 2021

**GOVERNMENT
AUDITING
STANDARDS**

2018 Revision

Technical Update April 2021

CMEP Practice Guide

The ERO Enterprise CMEP Practice Guide on Using the Work of Others provides specific guidance on who “others” can be as well as examples from the Standards.

CMEP staff will focus on the relevance of the materials provided as well as the independence and capabilities of those who provided the materials.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

This is a Compliance Monitoring and Enforcement Program (CMEP) Practice Guide. It is developed exclusively by the ERO Enterprise under its obligations for independence and objectivity. This CMEP Practice Guide is intended for use by ERO Enterprise Staff to support consistency as they perform CMEP activities. This CMEP Practice Guide is posted publicly solely to provide transparency.

ERO Enterprise CMEP Practice Guide

Using the Work of Others

March 14, 2023

Background
To support successful implementation and compliance with the North American Electric Reliability Corporation (NERC) Reliability Standards, the Electric Reliability Organization (ERO) Enterprise¹ adopted the Compliance Guidance Policy.² The Compliance Guidance Policy outlines the purpose, development, use, and maintenance of guidance for implementing Reliability Standards. According to the Compliance Guidance Policy, Compliance Guidance includes two types of guidance – (1) Implementation Guidance and (2) Compliance Monitoring and Enforcement Program (CMEP) Practice Guides.³ This document summarizes some of the requirements in NERC Reliability Standards, but the language of the Reliability Standards is enforceable and supersedes any description in this document.

Purpose
This CMEP Practice Guide provides guidance to CMEP staff⁴ when reviewing evidence, provided by registered entities, that is generated “Using the Work of Others.” Work of Others can include an assessment of the registered entity’s compliance with a Reliability Standard or an independent internal

Examples

Examples Already in the Standards

- Personnel Risk Assessments (CIP-004)
- Third-party Cyber Vulnerability Assessment (CVA) (CIP-010 R3)
- Vendor service risk assessments (CIP-011-3)
- Independent third-party assessment of vendors (CIP-013)
- Unaffiliated third-party reviews of risk assessments for physical security (CIP-014)

Other Examples

- FISMA audits
- Mock audits entities might perform for one another
- Certification Review for a new EMS
- Internal Audit teams at entities

When WECC Could Use the Work of Others

- WECC will evaluate the relevance of the materials provided to the audit objectives
- Acceptance will be case by case and will focus also on the independence of the others who provided the work
- The benefits are intended to be for the entity for work that the entity is already performing
- There is no requirement to use third parties to provide work

Internal Audit

Internal Audit

- Internal Audit is a primary example of using the work of others.
- The work of internal auditors can be an input to differentiate WECC's approach to audit and fieldwork.
- The concept is not “all or nothing” in the sense of replacing work WECC would otherwise do.
- The intent is not to re-perform the good work you have already done.
- WECC is not trying to free up time to audit more things; scopes will continue to be based on risk.



Electric Reliability and Security for the West

www.wecc.org