

Reliability Standard Audit Worksheet¹

CIP-002-5.1 — Cyber Security — BES Cyber System Categorization

This section to be completed by the Compliance Enforcement Authority.

Audit ID: Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity: Registered name of entity being audited
NCR Number: NCRnnnnn
Compliance Enforcement Authority: Region or NERC performing audit
Compliance Assessment Date(s)²: Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method: [On-site Audit | Off-site Audit | Spot Check]
Names of Auditors: Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	X	X	X	X				X			X	X		
R2	X	X	X	X	X				X			X	X		

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

¹ NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC’s and the Regional Entities’ assessment of a registered entity’s compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC’s Reliability Standards can be found on NERC’s website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity’s adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

² Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

DRAFT NERC Reliability Standard Audit Worksheet

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
R2			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

DRAFT NERC Reliability Standard Audit Worksheet

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

DRAFT

R1 Supporting Evidence and Documentation

- R1.** Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*
- i.** Control Centers and backup Control Centers;
 - ii.** Transmission stations and substations;
 - iii.** Generation resources;
 - iv.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
 - v.** Special Protection Systems that support the reliable operation of the Bulk Electric System; and
 - vi.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.
- 1.1.** Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;
- 1.2.** Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and
- 1.3.** Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).
- M1.** Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, and Parts 1.1 and 1.2.

Registered Entity Response (Required):

Question 1: Do you share compliance responsibility for this Requirement with another entity? Yes No

For example, is any BES Cyber System located at a shared facility?

If “Yes,” list the following for each asset for which compliance responsibility is shared:

- Asset name or designation
- Joint Registration Organization (JRO), Coordinated Functional Registration (CFR), or other document describing the shared compliance responsibility, if any
- Other information regarding the shared compliance responsibility which may be useful to the audit team in determining the appropriate audit scope and approach for the asset

Note: A separate spreadsheet or other document may be used to provide all or part of this information. If so, provide the document reference below.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of

DRAFT NERC Reliability Standard Audit Worksheet

compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-002-5.1, R1

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has a process to identify each high impact BES Cyber System, each medium impact BES Cyber System, and each asset that contains a low impact BES Cyber System.
	Verify the above process considers all of the following: <ul style="list-style-type: none"> i. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 of the Standard.
	Verify the entity has identified each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset.
	Verify the entity has identified each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset.
	Verify the entity has identified each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any.

Auditor Notes:

R2 Supporting Evidence and Documentation

- R2.** The Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*
- 2.1** Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and
 - 2.2** Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.
- M2.** Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

Registered Entity Response:

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-002-5.1, R2

This section to be completed by the Compliance Enforcement Authority

	Verify the reviews of the identifications in Requirement R1 have occurred at least once every 15 calendar months.
	Verify the approvals by the CIP Senior Manager or delegate of the identifications in Requirement R1 have occurred at least once every 15 calendar months.

Auditor Notes:

DRAFT

Additional Information:

Reliability Standard

The full text of CIP-002-5.1 may be found on the NERC Web Site (www.nerc.com) under “Program Areas & Departments”, “Reliability Standards.”

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

FERC Order No. 706

FERC Order No. 791

DRAFT NERC Reliability Standard Audit Worksheet

Revision History for RSAW

Version	Date	Reviewers	Revision Description
DRAFT1v0	06/17/2014	Posted for Industry Comment	New Document
DRAFT2v0	09/17/2014	CIP RSAW Development Team	Address comments received in response to DRAFT1v0.
DRAFT3v0	12/10/2014	CIP RSAW Development Team	Address comments received in response to DRAFT2v0.
DRAFT4v0	02/06/2015	CIP RSAW Development Team	Address comments from V5R SDT and address comments in response to DRAFT3v0.
DRAFT4v1	03/06/2015	CIP RSAW Development Team	Address comments from V5R SDT meeting on March 3-4, 2015.

DRAFT