NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-009-6 – Cyber Security – Security Management Controls

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		
R3	X	X	X	X	X				X			X	X		
R4	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.

Findings

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

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
P1.1			
P1.2			
P1.3			
P1.4			
P1.5			
R2			
P2.1			
P2.2			
P2.3			
R3			
P3.1			
P3.2			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

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)

R1 Supporting Evidence and Documentation

R1. Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in *CIP-009-6 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-6 Table R1 – Recovery Plan Specifications*.

R1 Part 1.1

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

Registered Entity Response (Required):
Question: Is R1 Part 1.1 applicable to this audit? ☐ Yes ☐ No
If "No," why not?
☐ This entity owns none of the systems listed in the "Applicable Systems" column of the Table for this Part.
☐ Other: [Provide explanation below]
[Note: A separate spreadsheet or other document may be used. 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented plan(s) for compliance with this Part.
List of all BES Cyber Systems identified as an Applicable System and identification of the corresponding

recovery plan(s).
List of all EACMS and PACS associated with each BES Cyber System identified as an Applicable System and identification of the corresponding recovery plan(s).
Identify the sections within the plan(s) that provide the conditions for the activation of the recovery plan(s).

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-009-6, R1 Part 1.1

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the plan(s) provide conditions for activation.
	Verify that for each Applicable System, there is a corresponding recovery plan.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.
	Assess the adequacy of the conditions provided; for any conditions deemed inadequate, provide reasons for the inadequacy and provide an Area of Concern or a Recommendation.

Note to Auditor:

1. Results-based Requirement: The auditor should note that this is a results-based Requirement. As such, the entity has great latitude in determining how the result is achieved. The auditor should focus on verifying that the result is complete and correct.

Auditor Notes:

R1 Part 1.2

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.

Registered Entity Response (Required):

Question: Is R1 Part 1.2 applicable to this audit? ☐ Yes ☐ No

If "No," why not?

☐ This entity owns none of the systems listed in the "Applicable Systems" column of the Table for this Part.

☐ Other: [Provide explanation below]

[Note: A separate spreadsheet or other document may be used. 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented plan(s) for compliance with this Part.
List of all BES Cyber Systems identified as an Applicable System and identification of the corresponding recovery plan(s).
List of all EACMS and PACS associated with each BES Cyber System identified as an Applicable System and identification of the corresponding recovery plan(s).
Identify the sections within the plan(s) that lists the roles of responders and responsibilities of each role.
Describe how individuals are associated with roles and how the association is kept current.

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-009-6, R1 Part 1.2

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify that for each Applicable System, there is a corresponding recovery plan.
	Verify the plan(s) identifies roles of responders.
	Verify the plan(s) identifies the responsibilities of each role.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.
	Review the description of how individuals are associated with roles and how the associations are kept current. An insufficiency in this area should be documented as an Area of Concern or a Recommendation.

Note to Auditor:

1. Results-based Requirement: The auditor should note that this is a results-based Requirement. As such, the entity has great latitude in determining how the result is achieved. The auditor should focus on verifying that the result is complete and correct.

Auditor Notes:

R1 Part 1.3

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

Registered Entity Response (Required):

Question: Is R1 Part 1.3 applicable to this audit? ☐ Yes ☐ No

If "No," why not?

☐ This entity owns none of the systems listed in the "Applicable Systems" column of the Table for this Part.

☐ Other: [Provide explanation below]

[Note: A separate spreadsheet or other document may be used. 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.

Initial Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented plans for compliance with this Part.
Identify the sections within the plan(s) that provide specific processes used for backing up and storing recovery information for each Applicable System.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System and identification of the corresponding recovery plan(s). 2. List of all EACMS and PACS associated with each BES Cyber System identified as an Applicable System and identification of the corresponding recovery plan(s).

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES

Cyber Systems, EACMS, and PACS to be used for the evidence requested below:
Evidence Set 2: 1. Evidence that each sampled BES Cyber System, EACMS, and PACS is being backed up. 2. Evidence that the information being backed up is sufficient to recover the functionality of the BES Cyber System, EACMS, or PACS. 3. Evidence that the backup information is stored.

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-009-6, R1 Part 1.3

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify that each Applicable System has a corresponding backup and storage process to recover BES Cyber System functionality.
	Verify the plan(s) or processes specify how information required for the restoration of an Applicable System will be backed up and restored.
	Verify the plan(s) or processes specify how the information stored for recovery will be ensured to be up-to-date to recover the functionality of the Applicable System.
	Verify that each sampled BES Cyber System, EACMS, and PACS is being backed up.
	Verify that the information being backed up is sufficient to recover the functionality of the BES Cyber System, EACMS, or PACS.
	Verify that the backup information is stored in accordance with the process.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.

Note to Auditor:

1. For the sampling of Evidence Set 1 to derive the list of systems which are the subject of Evidence Set 2, a judgmental sample is strongly recommended. The audit team should focus on higher risk systems, but not exclude all lower risk systems.

Auditor Notes:

R1 Part 1.4

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.

Registered Entity Response (Required):

Question: Is R1 Part 1.4 applicable to this audit? ☐ Yes ☐ No

If "No," why not?

☐ This entity owns none of the systems listed in the "Applicable Systems" column of the Table for this Part.

☐ Other: [Provide explanation below]

[Note: A separate spreadsheet or other document may be used. 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for compliance with this Part.
Identify the sections within the plan(s) that provide specific processes used to: 1. verify the successful completion of backups required to recover each Applicable System. 2. verify the storage of recovery information for each Applicable System. 3. address any backup failures.

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-009-6, R1 Part 1.4

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the plan(s) or processes specify how: 1. The successful completion of backups is verified. 2. Stored backup information is verified. 3. Backup failures are addressed.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R1 Part 1.5

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

Registered Entity Response (Required):

Question: Is R1 Part 1.5 applicable to this audit? ☐ Yes ☐ No

If "No," why not?

☐ This entity owns none of the systems listed in the "Applicable Systems" column of the Table for this Part.

☐ Other: [Provide explanation below]

[Note: A separate spreadsheet or other document may be used. 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for compliance with this Part.
List of all BES Cyber Systems identified as an Applicable System.
List of all BES Cyber Assets associated with each BES Cyber System identified as an Applicable System.
List of all EACMS and PACS associated with each BES Cyber System identified as an Applicable System.
Provide one or more specific processes per Cyber Asset type used to preserve data, per Cyber Asset capability.

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-009-6, R1 Part 1.5

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify that each Applicable System type has a corresponding specific process for the preservation of data to determine the cause of a Cyber Security Incident, per Cyber Asset capability.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.

Note to Auditor:

1. Results-based Requirement: The auditor should note that this is a results-based Requirement. As such, the entity has great latitude in determining how the result is achieved. The auditor should focus on verifying that the result is complete and correct.
2. When verifying processes for data preservation, note that processes may vary by Cyber Asset type. For example, all Windows 2008 servers of the same model and software may have one process for preserving data, but a network appliance may need to use a different process.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-6 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-6 Table R2 – Recovery Plan Implementation and Testing.*

R2 Part 2.1

CIP-009-6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

Registered Entity Response (Required):

Question: Is R2 Part 2.1 applicable to this audit? ☐ Yes ☐ No

If "No," why not?

☐ This entity owns none of the systems listed in the "Applicable Systems" column of the Table for this Part.

☐ Other: [Provide explanation below]

[Note: A separate spreadsheet or other document may be used. 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented plans for compliance with this Part.
List of all BES Cyber Systems identified as an Applicable System.

List of all BES Cyber Assets associated with each BES Cyber System identified as an Applicable System.
List of all EACMS and PACS associated with each BES Cyber System identified as an Applicable System.
Evidence, for every plan referenced in Requirement R1, of a test. For tests by: • Recovery from an actual incident, provide: o The date and time of the incident. o Logs showing the Applicable System's failure. o Evidence of the implementation of the recovery plan(s) including the results. o The date and time of the recovery. o Logs showing the Applicable System's recovery. o Personnel who performed the recovery. • Paper drill or tabletop exercise, provide: o The date and time of the drill or exercise. o Personnel who participated in the drill or exercise. o The conditions, content, and results of the drill or exercise. • Operational exercise, provide: o The date and time of the exercise. o Personnel who participated in the exercise. o The conditions, actions taken, and results of the exercise.

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-009-6, R2 Part 2.1

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify each plan provided in Requirement R1 has been tested at least once every 15 calendar months.
	For tests by: • Recovery from an actual incident: o Verify that the corresponding recovery plan(s) for the Applicable System were used in

	accordance with the plan(s). See Note 2. • Paper drill or tabletop exercise: o Verify that the participants of the drill or exercise have been documented in Requirement R1, Part 1.2. o Verify the drill or exercise was detailed and covered the content of the recovery plan(s). • Operational exercise: o Verify the participants of the exercise have been documented in Requirement R1, Part 1.2. o Verify that the exercise followed and executed the plan(s).
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.

Note to Auditor:

1. Results-based Requirement: The auditor should note that this is a results-based Requirement. As such, the entity has great latitude in determining how the result is achieved. The auditor should focus on verifying that the result is complete and correct.
2. Recovery from an actual incident should be corroborated by logs of the failed system, logs of the recovered system, and documentation of the use of the recovery plan.

Auditor Notes:

R2 Part 2.2

CIP-009-6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).

Registered Entity Response (Required):

Question: Is R2 Part 2.2 applicable to this audit? ☐ Yes ☐ No

If "No," why not?

☐ This entity owns none of the systems listed in the "Applicable Systems" column of the Table for this Part.

☐ Other: [Provide explanation below]

[Note: A separate spreadsheet or other document may be used. 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented plans for compliance with this Part.
List of all BES Cyber Systems identified as an Applicable System.
List of all BES Cyber Assets associated with each BES Cyber System identified as an Applicable System.
List of all EACMS and PACS associated with each BES Cyber System identified as an Applicable System.
Provide evidence that a representative sample of information used to recover Applicable Systems has been tested to ensure the information is useable and current.

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-009-6, R2 Part 2.2

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the entity's sample is representative of the information required to recover the Applicable Systems. See Note 2.
	Verify that the evidence provided ensures that the information is useable and that it matches the current configuration of the Applicable Systems: • The test should ensure that the information is not corrupt. • The test should ensure that the information is compatible with the current configuration. This may be corroborated by checking an Applicable System's change control logs and verifying that backup has taken place since any modifications that may impact backup information. • Other evidence for consideration: Logs of tools used to compare the information stored in backup matches the online configuration of the Applicable System. Evidence of an actual recovery including logs of the failed system, logs of the recovered system, and evidence of the use of the backed up information may be substituted for the above.
	Verify that the test has been performed at least once every 15 calendar months.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.

Note to Auditor:

1. Results-based Requirement: The auditor should note that this is a results-based Requirement. As such, the entity has great latitude in determining how the result is achieved. The auditor should focus on verifying that the result is complete and correct.
2. At least one of each type of an Applicable System's information and each type of storage media and system has been tested. For example, if there are Cisco and Juniper firewalls, then a representative sample should include testing of information for at least one Cisco and one Juniper firewall provided that all Cisco firewalls use similar software and their backups are performed and stored the same way and that all Juniper firewalls use similar software and their backups are performed and stored the same way.

Auditor Notes:

R2 Part 2.3

CIP-009-6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

Registered Entity Response (Required):
Question: Is R2 Part 2.3 applicable to this audit? ☐ Yes ☐ No
If "No," why not?
☐ This entity owns none of the systems listed in the "Applicable Systems" column of the Table for this Part.
☐ Other: [Provide explanation below]
[Note: A separate spreadsheet or other document may be used. 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for compliance with this Part.
List of all BES Cyber Systems identified as an Applicable System.
List of all BES Cyber Assets associated with each BES Cyber System identified as an Applicable System.
Provide dated evidence that each recovery plan identified in Requirement R1 has been tested either through an operational exercise in an environment that is representative of the production environment or through an actual recovery operation.

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-009-6, R2 Part 2.3

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify that each plan identified in Requirement R1 has been tested at least once every 36 calendar months.
	Verify the test for each plan identified in Requirement R1 meets the following: • For each test that used an operational exercise: o Verify the environment is representative of the the production environment that it is being used to test. For example, recovery of an EMS server should be performed on the same type of server hardware running the same versions of firmware. In the case of virtual servers, the hypervisor, allocated memory, and other resources on the test environment should match the EMS server's virtual environment. Note: Virtual environments should not substitute for traditional hardware/software environments and vice versa. o Verify that the documentation provided shows specific actions that were performed in the test and that the recovery plan was followed. • For each test that used an actual recovery: o Verify that the documentation provided shows specific actions that were performed in the recovery and that the recovery plan was followed.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.

Note to Auditor:

1. Results-based Requirement: The auditor should note that this is a results-based Requirement. As such, the entity has great latitude in determining how the result is achieved. The auditor should focus on verifying that the result is complete and correct.

Auditor Notes:

R3 Supporting Evidence and Documentation

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in *CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication.*

R3 Part 3.1

CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

Registered Entity Response (Required):

Question: Is R3 Part 3.1 applicable to this audit? ☐ Yes ☐ No

If "No," why not?

☐ This entity owns none of the systems listed in the "Applicable Systems" column of the Table for this Part.

☐ Other: [Provide explanation below]

[Note: A separate spreadsheet or other document may be used. 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented plans for compliance with this Part.
List of all BES Cyber Systems identified as an Applicable System.
List of all BES Cyber Assets associated with each BES Cyber System identified as an Applicable System.
List of all EACMS and PACS associated with each BES Cyber System identified as an Applicable System.
List of an actual recovery of Applicable Systems.
Provide dated documented evidence of any lessons learned or the absence of any lessons learned as a result of all recovery plan tests or an actual recovery.
Provide dated evidence of updates to any recovery plan(s) as result of any documented lessons learned.
Provide dated evidence that each person or group with a defined role in the recovery plan(s) has been notified of all updates to the recovery plan(s) due to any documented lessons learned.
For plan(s) that have identified roles and responsibilities by groups, provide the individual members of each group.

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-009-6, R3 Part 3.1
This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify for each time a recovery plan has been exercised either as a test or an actual recovery, that within 90 calendar days, there is a documentation of lessons learned or the absence of lessons learned. At a

	minimum, this should be corroborated with the list of tests required in Requirement R2 and to any actual recoveries.
	Verify for any documented lessons learned, within 90 calendar days, that all applicable recovery plan(s) have been updated. See Note 2.
	Verify that within 90 calendar days of a recovery, that any updates to a recovery plan resulting from a documented lessons learned, have been communicated to all persons or group (and each member of the group) with a defined role in the recovery plan. See Note 3.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.

Note to Auditor:

1. Results-based Requirement: The auditor should note that this is a results-based Requirement. As such, the entity has great latitude in determining how the result is achieved. The auditor should focus on verifying that the result is complete and correct.
2. Recovery plans other than the identified plan should be evaluated for susceptibility to the same issues identified in the lessons learned. For example, if the lessons learned identified that recovery fails to a Windows server because a network sentry blocks one of the recovery files in transit, the recovery plan not only for the Windows servers, but also Windows workstations that rely on the same file, should be updated to correct the failed recovery.
3. This notification should be corroborated through Requirement R1, Part 1.2 such that all individuals who have a role in the recovery operation have been made aware of any updates.

Auditor Notes:

R3 Part 3.2

CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

Registered Entity Response (Required):
Question: Is R3 Part 3.2 applicable to this audit? ☐ Yes ☐ No
If "No," why not?
☐ This entity owns none of the systems listed in the "Applicable Systems" column of the Table for this Part.
☐ Other: [Provide explanation below]
[Note: A separate spreadsheet or other document may be used. 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented plans for compliance with this Part.
List of all BES Cyber Systems identified as an Applicable System.
List of all BES Cyber Assets associated with each BES Cyber System identified as an Applicable System.

List of all EACMS and PACS associated with each BES Cyber System identified as an Applicable System.
Provide dated evidence that each recovery plan identified in Requirement R1 was updated for any changes to the roles and responsibilities, responders, or technology deemed impactful to the recovery plan.
Provide dated evidence that any updates to the recovery plan(s) were communicated to each person or group with a defined role in the recovery plan(s).
For plan(s) that have identified roles and responsibilities by groups, provide the individual members of each group.

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-009-6, R3 Part 3.2

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify that within 60 calendar days of any changes to the roles and responsibilities, responders, or technology deemed impactful to the recovery plan(s), the recovery plan(s) were updated. See Note 2.
	Verify that within 60 calendar days of any changes to the roles and responsibilities, responders, or technology deemed impactful to the recovery plan(s), any updates to the plan(s) were communicated to each person or group (and each member of the group) with a defined role in the recovery plan(s).
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.

Note to Auditor:

1. Results-based Requirement: The auditor should note that this is a results-based Requirement. As such, the entity has great latitude in determining how the result is achieved. The auditor should focus on verifying that the result is complete and correct.
2. Corroborate evidence provided with versions of the plan(s) and the documented lessons learned from Requirement R3, Part 3.1.1, if any.

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-009-6 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

See FERC Order 706
See FERC Order 791

Selected Glossary Terms

The following Glossary terms are provided for convenience only. Please refer to the NERC web site for the current enforceable terms.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
Draft1v0	06/17/2014	Posted for Industry Comment	New Document

[i] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.