NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Reliability Standard Audit Worksheet[1]

## CIP-009-6 – Cyber Security – Recovery Plans for BES Cyber Systems

***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:<br>1. EACMS; and<br>2. PACS<br><br>Medium Impact BES Cyber Systems and their associated:<br>1. EACMS; and<br>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]

**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 compliance may be found.** | | | | | |
|---|---|---|---|---|---|
| **File Name** | **Document Title** | **Revision or** | **Document Date** | **Relevant Page(s)** | **Description of Applicability of Document** |

| | | Version | | or Section(s) | |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |

**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***

| | |
|---|---|
| | Verify the plan(s) have conditions for activation of the recovery plan(s). |

**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:<br>1. EACMS; and<br>2. PACS<br><br>Medium Impact BES Cyber Systems and their associated:<br>1. EACMS; and<br>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]

**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 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***

| | |
|---|---|
| | Verify the plan(s) have roles and responsibilities of responders. |

**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:<br>1. EACMS; and<br>2. PACS<br><br>Medium Impact BES Cyber Systems and their associated:<br>1. EACMS; and<br>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]

**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 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***

| | |
|---|---|
| | Verify the plan(s) have one or more processes for the backup and storage of information required to recover BES Cyber System functionality. |

**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:<br>1. EACMS; and<br>2. PACS<br><br>Medium Impact BES Cyber Systems at Control Centers and their associated:<br>1. EACMS; and<br>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]

**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 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***

| | |
|---|---|
| | Verify the plan(s) have one or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures. |

**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:<br>1. EACMS; and<br>2. PACS<br><br>Medium Impact BES Cyber Systems and their associated:<br>1. EACMS; and<br>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]

**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 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***

| | |
|---|---|
| | Verify the plan(s) have 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). |

**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:<br>1. EACMS; and<br>2. PACS<br><br>Medium Impact BES Cyber Systems at Control Centers and their associated:<br>1. EACMS; and<br>2. PACS | Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months:<br>• By recovering from an actual incident;<br>• With a paper drill or tabletop exercise; or<br>• 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]

**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 compliance may be found.** | | | | | |
|---|---|---|---|---|---|
| **File Name** | **Document Title** | **Revision or** | **Document Date** | **Relevant Page(s)** | **Description of Applicability of Document** |

| | | Version | | or Section(s) | |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |

**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***

| | |
|---|---|
| | Verify the Responsible Entity has tested each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months:<br>• By recovering from an actual incident;<br>• With a paper drill or tabletop exercise; or<br>• With an operational exercise. |

**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:<br>1. EACMS; and<br>2. PACS<br><br>Medium Impact BES Cyber Systems at Control Centers and their associated:<br>1. EACMS; and<br>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.<br><br>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]

**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 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***

| | |
|---|---|
| | Verify the Responsible Entity has tested 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. |

**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.<br><br>An actual recovery response may substitute for an operational exercise. | Examples of evidence may include, but are not limited to, dated documentation of:<br>• An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or<br>• 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]

**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 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***

| | |
|---|---|
| | Verify the Responsible Entity has tested 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. |

**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:<br>1. EACMS; and<br>2. PACS<br><br>Medium Impact BES Cyber Systems at Control Centers and their associated:<br>1. EACMS; and<br>2. PACS | No later than 90 calendar days after completion of a recovery plan test or actual recovery:<br>3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned;<br>3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and<br>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:<br>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;<br>2. Dated and revised recovery plan showing any changes based on the lessons learned; and<br>3. Evidence of plan update distribution including, but not limited to:<br>• Emails;<br>• USPS or other mail service;<br>• Electronic distribution system; or<br>• 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]

**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 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***

| | |
|---|---|
| | Verify that no later than 90 calendar days after completion of a recovery plan test or actual recovery, the Responsible Entity has:<br>3.1.1. Documented any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned;<br>3.1.2. Updated the recovery plan based on any documented lessons learned associated with the plan; and<br>3.1.3. Notified 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. |

**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:<br>1. EACMS; and<br>2. PACS<br><br>Medium Impact BES Cyber Systems at Control Centers and their associated:<br>1. EACMS; and<br>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:<br>3.2.1. Update the recovery plan; and<br>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:<br>1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and<br>2. Evidence of plan update distribution including, but not limited to:<br>• Emails;<br>• USPS or other mail service;<br>• Electronic distribution system; or<br>• 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]

**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 compliance may be found.** | | | | | |
|---|---|---|---|---|---|
| **File Name** | **Document Title** | **Revision or Version** | **Document Date** | **Relevant Page(s) or** | **Description of Applicability of Document** |

| | | | | Section(s) | |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |

**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***

| | |
|---|---|
| | Verify that 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, the Responsible Entity has:<br>3.2.1. Updated the recovery plan; and<br>3.2.2. Notified each person or group with a defined role in the recovery plan of the updates. |

**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

## Revision History for RSAW

| Version | Date | Reviewers | Revision Description |
|---|---|---|---|
| DRAFT1v0 | 06/17/2014 | Posted for Industry Comment | New Document |
| DRAFT2v0 | 9/17/2014 | 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. |
| | | | |