

**Reliability Standard Audit Worksheet for British Columbia**

CIP-009-5 – Cyber Security – Recovery Plans for BES Cyber Systems

Reliability Standard Effective Date for BC: October 1, 2018

***The Compliance Monitor Administrator must complete this section***

**Registered Entity:** [Name & ACRO]

**WCR Number:** WCRXXXXX

**Compliance Assessment Date:** [Audit start date – audit end date]

**Compliance Monitoring Method:** [Audit Type]

**Applicable Function(s):** BA, DP, GO, GOP, TO, TOP

**Names of Auditors:**

Findings Table:

|  |  |  |  |
| --- | --- | --- | --- |
| Req. | Finding | Summary and Documentation | Functions Monitored |
| [R1](#R1_Summary) |  |  | BA, DP, GO, GOP, TO, TOP |
| [R2](#R2_Summary) |  |  | BA, DP, GO, GOP, TO, TOP |
| [R3](#R3_Summary) |  |  | BA, DP, GO, GOP, TO, TOP |

|  |  |
| --- | --- |
| Req. | Areas of Concern |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
| Req. | Recommendations |
|  |  |
|  |  |
|  |  |

# **Subject Matter Experts**

Identify subject matter expert(s) responsible for this Reliability Standard. Insert additional lines if necessary.

**Registered Entity Response (Required):**

|  |  |  |  |
| --- | --- | --- | --- |
| **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-009-5 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-009-5 Table R1 – Recovery Plan Specifications*.

| **CIP-009-5 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):**

Describe, in narrative form, how you meet compliance with this requirement.

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 Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 1.1

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more recovery plans which include conditions for activation of the recovery plan(s). |

| **CIP-009-5 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):**

Describe, in narrative form, how you meet compliance with this requirement.

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 Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 1.2

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more recovery plans which include roles and responsibilities of responders. |

| **CIP-009-5 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):**

Describe, in narrative form, how you meet compliance with this requirement.

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** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Compliance Assessment Approach Specific to Part 1.3

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more recovery plans which include one or more processes for the backup and storage of information required to recover BES Cyber System functionality. |

| **CIP-009-5 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):**

Describe, in narrative form, how you meet compliance with this requirement.

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 Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 1.4

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more recovery plans which include one or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures. |

| **CIP-009-5 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):**

Describe, in narrative form, how you meet compliance with this requirement.

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 Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 1.5

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more recovery plans which include 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. |

**[Compliance Summary:](#R1)**

|  |
| --- |
| Finding Summary:Primary Documents Supporting Findings: |

**Auditor Notes:**

|  |
| --- |
|  |

**R2 Supporting Evidence and Documentation**

**R2.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-5 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-009-5 Table R2 – Recovery Plan Implementation and Testing.*

| **CIP-009-5 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):**

Describe, in narrative form, how you meet compliance with this requirement.

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 Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 2.1

***This section to be completed by the Compliance Monitor Administrator***

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

| **CIP-009-5 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):**

Describe, in narrative form, how you meet compliance with this requirement.

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 Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 2.2

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | For each recovery plan, verify either: * 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; or
* the Responsible Entity has performed an actual recovery that incorporates the information used to recover BES Cyber System functionality.
 |

| **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):**

Describe, in narrative form, how you meet compliance with this requirement.

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 Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 2.3

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | For each recovery plan, verify either: * 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; or
* the Responsible Entity has performed an actual recovery response.
 |

**[Compliance Summary:](#R2)**

|  |
| --- |
| Finding Summary:Primary Documents Supporting Findings: |

**Auditor Notes:**

|  |
| --- |
|  |

**R3 Supporting Evidence and Documentation**

**R3.** Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable requirement parts in *CIP-009-5 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-009-5 Table R3 – RecoveryPlan Review, Update and Communication.*

| **CIP-009-5 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:1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned;
2. Update the recovery plan based on any documented lessons learned associated with the plan; and
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):**

Describe, in narrative form, how you meet compliance with this requirement.

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 Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 3.1

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify that no later than 90 calendar days after completion of a recovery plan test or actual recovery, the Responsible Entity has:1. Documented any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned;
2. updated the recovery plan based on any documented lessons learned associated with the plan; and
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.
 |

| **CIP-009-5 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:1. Update the recovery plan; and
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):**

Describe, in narrative form, how you meet compliance with this requirement.

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 Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 3.2

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | 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:1. Updated the recovery plan; and
2. notified each person or group with a defined role in the recovery plan of the updates.
 |

**[Compliance Summary:](#R3)**

|  |
| --- |
| Finding Summary:Primary Documents Supporting Findings: |

**Auditor Notes:**

|  |
| --- |
|  |

**Revision History for RSAW**

|  |  |  |
| --- | --- | --- |
| **Date** | **Reviewer(s)** | **Revision Description** |
| 3/7/2016 | Jennifer Salisbury, WECCJulie Blair, WECCWECC CIP SME | Intial version  |
|  |  |  |
|  |  |  |