

**Reliability Standard Audit Worksheet for British Columbia**

# CIP-010-1 – Cyber Security – Configuration Change Management & Vulnerability Assessments

# 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)** |  |  | BA, DP, GO, GOP, TO, TOP |
| **[R2](#R2)** |  |  | BA, DP, GO, GOP, TO, TOP |
| **[R3](#R3)** |  |  | 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 implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

**M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| **CIP-010-1 Table R1 – Configuration Change Management** | | | |
| --- | --- | --- | --- |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.1 | High Impact BES Cyber Systems and their associated:   1. EACMS; 2. PACS; and 3. PCA   Medium Impact BES Cyber Systems and their associated:   1. EACMS; 2. PACS; and 3. PCA | Develop a baseline configuration, individually or by group, which shall include the following items:   1. Operating system(s) (including version) or firmware where no independent operating system exists; 2. Any commercially available or open-source application software (including version) intentionally installed; 3. Any custom software installed; 4. Any logical network accessible ports; and 5. Any security patches applied. | Examples of evidence may include, but are not limited to:   * A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or * A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group. |

**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 that the Responsible Entity has documented one or more processes that include the development of a baseline configuration for each Applicable System. |
|  | For each Applicable System, verify the above documented process(es) collectively include all of the following:   1. Operating system(s) (including version) or firmware where no independent operating system exists; 2. any commercially available or open-source application software (including version) intentionally installed; 3. any custom software installed; 4. any logical network accessible ports; and 5. any security patches applied. |
|  | Verify the Responsible Entity has a baseline configuration for each Applicable System, individually or by group, which includes:   1. Operating system(s) (including version) or firmware where no independent operating system exists; 2. any commercially available or open-source application software (including version) intentionally installed; 3. any custom software installed; 4. any logical network accessible ports; and 5. any security patches applied. |

| **CIP-010-1 Table R1 – Configuration Change Management** | | | |
| --- | --- | --- | --- |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.2 | High Impact BES Cyber Systems and their associated:   1. EACMS; 2. PACS; and 3. PCA   Medium Impact BES Cyber Systems and their associated:   1. EACMS; 2. PACS; and 3. PCA | Authorize and document changes that deviate from the existing baseline configuration. | Examples of evidence may include, but are not limited to:   * A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or * Documentation that the change was performed in accordance with the requirement. |

**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 documented one or more processes to authorize and document changes that deviate from the existing baseline configuration. |
|  | For each Applicable System, verify the Responsible Entity authorized and documented changes that deviate from the existing baseline configuration. |

| **CIP-010-1 Table R1 – Configuration Change Management** | | | |
| --- | --- | --- | --- |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.3 | High Impact BES Cyber Systems and their associated:   1. EACMS; 2. PACS; and 3. PCA   Medium Impact BES Cyber Systems and their associated:   1. EACMS; 2. PACS; and 3. PCA | For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change. | An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change. |

**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 1.3

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

|  |  |
| --- | --- |
|  | For a change that deviates from the existing baseline configuration, verify the Responsible Entity documented one or more processes for updating the baseline configuration as necessary within 30 calendar days of completing the change. |
|  | For each Applicable System, for a change that deviates from the existing baseline configuration, verify the Responsible Entity updated the baseline configuration as necessary within 30 calendar days of completing the change. |

| **CIP-010-1 Table R1 – Configuration Change Management** | | | |
| --- | --- | --- | --- |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.4 | High Impact BES Cyber Systems and their associated:   1. EACMS; 2. PACS; and 3. PCA   Medium Impact BES Cyber Systems and their associated:   1. EACMS; 2. PACS; and 3. PCA | For a change that deviates from the existing baseline configuration:   1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 3. Document the results of the verification. | An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results. |

**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***

|  |  |
| --- | --- |
|  | For a change that deviates from the existing baseline configuration, verify the Responsible Entity documented one or more processes to:   1. Determine, prior to the change, required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 2. verify, following the change, that required cyber security controls determined in Part 1.4.1 are not adversely affected; and 3. document the results of the verification. |
|  | For each change that deviates from the existing baseline configuration, for each Applicable System, verify that:   1. Prior to the change, the Responsible Entity has determined the required security controls in CIP-005 and CIP-007 that could be impacted by the change; 2. following the change, the Responsible Entity has verified that the required cyber security controls determined in 1, above, are not adversely affected; and 3. the Responsible Entity has documented the results of the verification required by 2, above. |

| **CIP-010-1 Table R1 – Configuration Change Management** | | | |
| --- | --- | --- | --- |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.5 | High Impact BES Cyber Systems | Where technically feasible, for each change that deviates from the existing baseline configuration:   1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments. | An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test. |

**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***

|  |  |
| --- | --- |
|  | For changes that deviate from the existing baseline configuration, verify the Responsible Entity documented one or more processes that include:   1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 2. document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments. |
|  | Verify that, for each Applicable System, for each change that deviates from the existing baseline configuration, prior to implementing any change in the production environment:   * The Responsible Entity tested the changes in a test environment; or * the Responsible Entity tested the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; or * a TFE covers this circumstance. |
|  | Verify that, for each Applicable System, where technically feasible, for each change that deviates from the existing baseline configuration, verify:   1. The Responsible Entity documented the results of the testing; and 2. if a test environment was used, the Responsible Entity documented the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments. |
|  |  |
| **Note to Auditor:**  The Responsible Entity may maintain a document describing the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments, rather than documenting these differences for every change. If this is the case, this document should be referenced by the change documentation, and may be reviewed by the audit team as part of the change documentation. | |

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

|  |
| --- |
| 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, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

**M2.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table*.*

| **CIP-010-1 Table R2 – Configuration Monitoring** | | | |
| --- | --- | --- | --- |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 2.1 | High Impact BES Cyber Systems and their associated:   1. EACMS; and 2. PCA | Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes. | An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected. |

**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 documented one or more processes to monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). |
|  | Verify the Responsible Entity documented one or more processes to document and investigate detected unauthorized changes. |
|  | For each Applicable System, verify the Responsible Entity monitored at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). |
|  | For each Applicable System, verify all detected unauthorized changes were documented and investigated. |

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

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

**Auditor Notes:**

|  |
| --- |
|  |

# **R3 Supporting Evidence and Documentation**

**R3.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

**M3.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table*.*

| **CIP-010-1 Table R3 – Vulnerability Assessments** | | | |
| --- | --- | --- | --- |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 3.1 | High Impact BES Cyber Systems and their associated:   1. EACMS; 2. PACS; and 3. PCA   Medium Impact BES Cyber Systems and their associated:   1. EACMS; 2. PACS; and 3. PCA | At least once every 15 calendar months, conduct a paper or active vulnerability assessment. | Examples of evidence may include, but are not limited to:   * A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment,; or * A document listing the date of the assessment and the output of any tools used to perform the assessment. |

**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 the Responsible Entity documented one or more processes for conducting a paper or active vulnerability assessment at least once every 15 calendar months. |
|  | For each Applicable System, verify the Responsible Entity conducted a paper or active vulnerability assessment at least once every 15 calendar months. |

| **CIP-010-1 Table R3 – Vulnerability Assessments** | | | | |
| --- | --- | --- | --- | --- |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 3.2 | High Impact BES Cyber Systems | Where technically feasible, at least once every 36 calendar months:   1. Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments. | An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment. |

**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 the Responsible Entity documented one or more processes to:   1. Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 2. document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments. |
|  | For each Applicable System, was an active vulnerability assessment technically feasible?   * If yes, verify:   + An active vulnerability assessment was conducted at least once every 36 calendar months, in accordance with 3.2.1; and   + results of testing are documented, in accordance with 3.2.2. * If no, verify the compensating measures identified by the TFE are implemented. |

| **CIP-010-1 Table R3 – Vulnerability Assessments** | | | |
| --- | --- | --- | --- |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 3.3 | High Impact BES Cyber Systems and their associated:   1. EACMS; 2. PCA | Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset. | An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment. |

**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 3.3

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

|  |  |
| --- | --- |
|  | Verify the Responsible Entity documented one or more processes for performing an active vulnerability assessment, prior to adding a new applicable Cyber Asset to a production environment, of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset. |
|  | For each Applicable System, was a new applicable Cyber Asset added to a production environment? If yes, verify that an active vulnerability assessment of the new Cyber Asset was performed prior to adding it to a production environment, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset. |
|  | If the Responsible Entity has experienced an exception for CIP Exceptional Circumstances, verify the Responsible Entity has adhered to any applicable cyber security policies. |
| **Note to Auditor:**  The Responsible Entity may reference a separate set of documents to demonstrate its response to any requirements impacted by CIP Exceptional Circumstances. | |

| **CIP-010-1 Table R3 – Vulnerability Assessments** | | | |
| --- | --- | --- | --- |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 3.4 | High Impact BES Cyber Systems and their associated:   1. EACMS; 2. PACS; and 3. PCA   Medium Impact BES Cyber Systems and their associated:   1. EACMS; 2. PACS; and 3. PCA | Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items. | An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items). |

**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 3.4

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

|  |  |
| --- | --- |
|  | Verify the Responsible Entity documented one or more processes to document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items. |
|  | For each Applicable System, for each assessment conducted according to Parts 3.1, 3.2, and 3.3, verify the results of the assessment were documented. |
|  | For each Applicable System, for each assessment conducted according to Parts 3.1, 3.2, and 3.3, were any vulnerabilities identified?  If yes, verify:   1. An action plan to remediate or mitigate the identified vulnerabilities was created or modified; 2. the action plan includes a planned date of completion; 3. the action plan includes the execution status of any remediation or mitigation action items; 4. the status of the action plan, if the planned date of completion has been exceeded; and 5. the completion of the action plan, if the action plan status is complete. |

**[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, WECC  Julie Blair, WECC  WECC CIP SME | Intial version |
|  |  |  |
|  |  |  |