NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Technical Reference Document

BCSI in the Cloud Tabletop Exercise

March 22, 2023

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

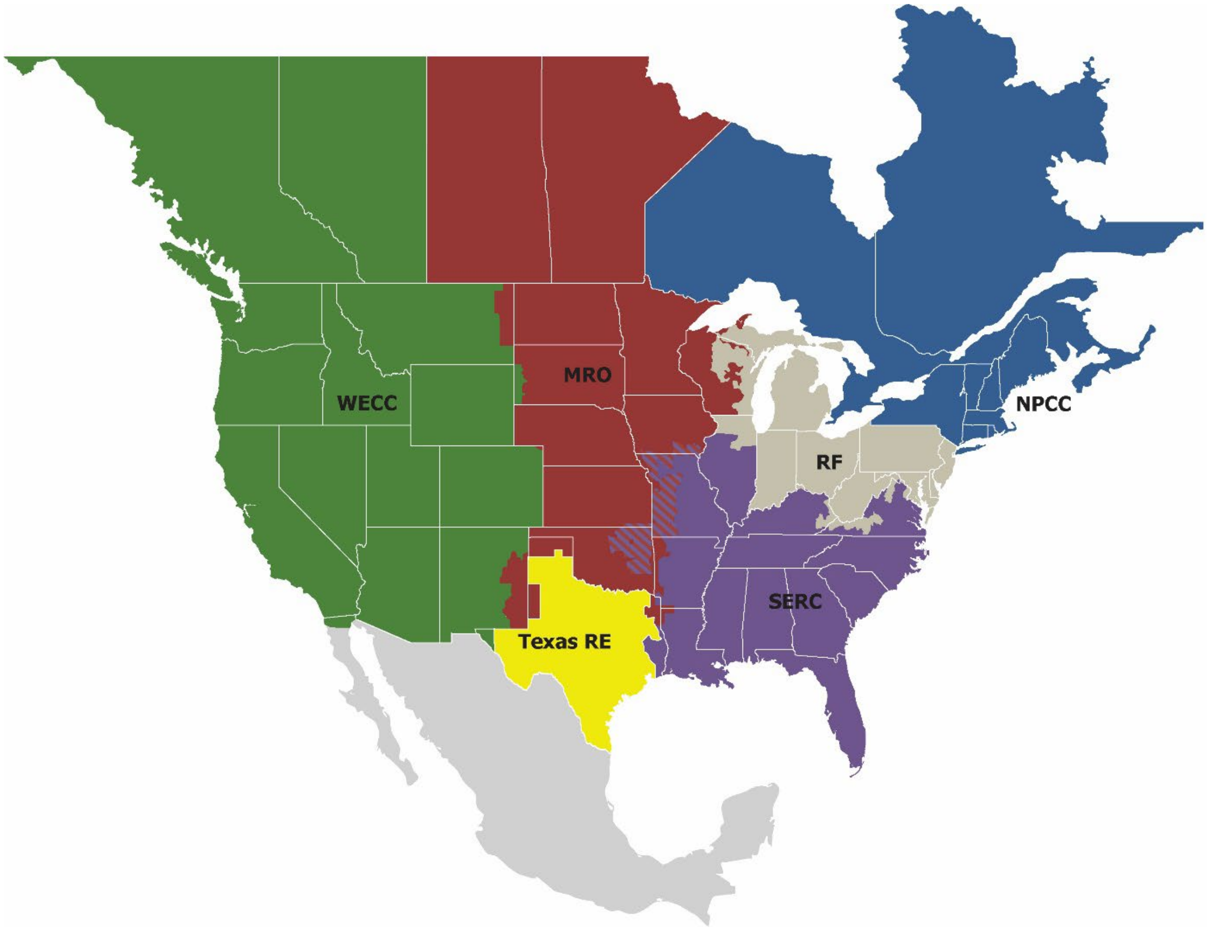
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of NERC and the six Regional Entities, is a highly reliable, resilient, and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entity boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Executive Summary

This document, designed to convey experiences learned from the NERC Security Working Group (SWG) and ERO Enterprise BCSI tabletop exercise, is not intended to establish new requirements under NERC's Reliability Standards, modify the requirements in any existing reliability standards, or provide an Interpretation under Section 7 of the Standard Processes Manual. Additionally, there may be other legitimate ways to fulfill the obligations of the requirements that are not expressed within this supporting document. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standard.

Primary Interest Groups

- Balancing Authority (BA)
- Distribution Provider (DP)
- Generator Operator (GOP)
- Generator Owner (GO)
- Reliability Coordinator (RC)
- Transmission Operator (TOP)
- Transmission Owner (TO)

Introduction

Industry interest in adopting commercially available cloud environments continues to increase substantially. FERC's Notice of Inquiry (NOI) sought comments regarding the potential benefits and risks associated with the use of virtualization and cloud computing services in association with bulk electric system operations, as well as whether barriers exist in the Commission-approved Critical Infrastructure Protection (CIP) Reliability Standards that impede the voluntary adoption of virtualization or cloud computing services.

Compliance Enforcement Authorities (CEA) and entities are challenged by how to evaluate and audit security controls for BES Cyber System Information (BCSI) stored in a cloud service provider (CSP) off premise environment, where a responsible entity or CEA does not have physical access to the BCSI storage system at a CSP's data center and CSP personnel potentially have logical access to such data.

On a more basic level, more information is needed for responsible entities, Regional Entities, the ERO, and FERC about how to prepare for an audit of an information protection program that includes repositories in a cloud environment.

The following efforts and work products are related to virtualization and cloud computing (specifically around BCSI and not BES operations):

- NERC Standards Project 2016-02: Virtualization[1]
  - *CIP V5 Issues for Standard Drafting Team Consideration* [2]
- NERC Standards Project 2019-02: BCSI Access Management[3]
- ERO Enterprise *Compliance Monitoring and Enforcement Program Practice Guide: BES Cyber System Information*[4]
- NERC Security Guideline: *Supply Chain Risks Related to Cloud Service Providers*[5]
- NERC Security Guideline: *Primer for Cloud Solutions and Encrypting BCSI*[6]
- FERC NOI on *Virtualization and Cloud Computing Services*[7]
  - Comments on FERC NOI on Virtualization and Cloud Computing Services[8]

This purpose in this lesson learned document is to continue in these efforts and create an awareness of the considerations made and ensure controls are commensurate with the risks.

[1] https://www.nerc.com/pa/Stand/Pages/Project%202016-02%20Modifications%20to%20CIP%20Standards.aspx

[2] https://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/Transfer_Issues_V5TAG-SDT_1st-final-03232016.pdf

[3] https://www.nerc.com/pa/Stand/Pages/Project2019-02BCSIAccessManagement.aspx

[4] https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/ERO%20Enterprise%20CMEP%20Practice%20Guide%20_%20BCSI%20-%20v0.2%20CLEAN.pdf

[5] https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Cloud_Computing.pdf

[6] https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline_BCSI_Cloud_Encryption.pdf

[7] https://www.ferc.gov/sites/default/files/2020-05/E-19_6.pdf

[8] https://elibrary.ferc.gov/eLibrary/docketsheet?docket_number=RM20-8&Subdocket=All&dtFrom=1960-01-01&dtTo=2020-12-18&chklegadata=false&PageNm=dsearch&dateRange=custom&searchType=docket&dateType=filed_date&sub_docket_Q=Allsub

Chapter 1: Tabletop Exercise Strategy

There is a lack of practical experience implementing, monitoring, and demonstrating compliance with the current NERC CIP Standards for BCSI cloud-based storage. Recognizing the myriad of ways a cloud environment can be implemented and managed using a consistent process to validate and/or test controls for BCSI in a cloud environment is imperative to ensuring the confidentiality of BCSI in a CSP environment.

Create and Test a Consistent Process for Evaluating a Cloud Environment

The first part of the strategy is to provide a consistent process for evaluating the compliance of a particular cloud environment. The SWG developed an initial process document for performing a tabletop exercise that mimics actual audit conditions. As more tabletops are performed, the process itself can be optimized for efficient use. The process is vendor neutral. The process document itself is managed by the SWG and will be updated on a regular basis. This technical reference document represents the first tabletop exercise performed using the SWG process document.

Use the Tabletop Process to Learn

The second part of the strategy is for a responsible entity (including its CSP) and the ERO Enterprise to use the process for a particular cloud implementation (IaaS, PaaS, SaaS), and pass on the experience to the industry. Over time, a knowledgebase is developed, and common best practices will emerge for both the ERO Enterprise and industry. Essentially, the process becomes repeatable and educates the ERO and industry about potentially successful approaches for meeting security objectives for NERC CIP Standards applicable in the cloud environments and successfully managing cloud-centric risks. Tabletop exercises should also produce a more accurate picture of how the audit process will realistically work, similar to a mock audit, which exercises processes such as interviews as well as the examination of the compliance evidence itself.

Technical Reference Deliverables

The process document addresses what the technical reference package will contain, e.g. the updated process document, categories of evidence provided, key auditor and/or risk management questions, etc. Driven by the process document, the deliverable packages will provide consistent information from exercise to exercise. **Use of the process and/or the deliverables provided by the process does not guarantee demonstration of compliance for any particular entity.**

Appendix A shows the relationship between the four documents in the deliverable package. The charts help simplify the navigation steps as package is read, with the arrows showing the suggested order to read the documents based on starting with the results or starting with the process.

Appendix B is a table showing a detailed cross-reference of evidence, standards/requirements, and description which maps into the ERO Enterprise document *BCSI Cloud Storage Tabletop Exercise; Slide 24 Appendix A - Exercise Evidence Mapping* that is included in this PDF package. The ERO Enterprise document also references to this Appendix B.

Process Participants

The process calls for the CSP, responsible entity, and the ERO Enterprise to participate so all three organizations can learn from all perspectives and ensure a more effective audit and value for other Compliance Monitoring and Enforcement Program (CMEP) activities involving cloud environments.

Chapter 2: Initial Tabletop Exercise

This exercise provided a review of BCSI in a CSP environment for the participating responsible entity, ERO Enterprise, and CSPs seeking to serve the electric sector. The exercise created the following value:

- Providing NERC and industry with possible security controls available for responsible entities storing BCSI at non-entity locations, e.g. the CSP data center
- Experience to develop guidance and audit approaches for responsible entities considering storage of BCSI in a CSP environment. The current standards do not specifically address BCSI in CSP environments and the Reliability Standards under development could leverage the experiences from this exercise.
- Providing industry and the ERO Enterprise with considerations for interpretation of existing NERC CIP Standards and what security considerations may be required in the future.
- Allowing the participating responsible entity to collaborate with the ERO Enterprise and CSP to establish a test audit scenario for cloud storage of BCSI.
- Provided the ERO Enterprise a live display of what controls can be utilized to protect cloud hosted BCSI as well as what evidence artifacts could demonstrate meeting and exceeding an audit.
- Helps industry to address shared responsibly model issues between entities and cloud providers.
- Provided context with the *ERO Enterprise CMEP Practice Guide for BES Cyber System Information*.[9]

[9] https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/ERO Enterprise CMEP Practice Guide   BCSI - v0.2 CLEAN.pdf

Chapter 3: Time and Resources (Estimated)

1. Total participants in the four hour exercise: 22 people
   a. 3 from Microsoft
   b. 14 from the responsible entity
   c. 5 from the ERO Enterprise, including NERC, WECC, and MRO
   d. NOTE: Not all participants were needed for the entire four hours from the responsible entity
2. Hours of effort for preparation activities for the responsible entity: 48 hours
   a. About four of those hours were shared between the responsible entity and Microsoft. Microsoft had their documentation already prepared.
3. Hours of effort for follow-up activities for the responsible entity: 40 hours
4. Total data request questions (after action activity): 20
5. Number of evidence files produced: 75
6. This exercise was Version 1.0. The intent behind the Technical Reference deliverables is to reduce preparation time for the responsible entity, the CSP, and ERO Enterprise by not having to produce the process and TRDs from scratch. The more the tabletop process is exercised, the more can be learned from it and efficiencies can be gained though better preparation, better questions/answers, and better understanding

Chapter 4: Tabletop Exercise

Responsible Entity Tabletop using Microsoft Azure

In May 2020, a tabletop exercise was conducted for BCSI in the Cloud as part of an activity coordinated with the SWG. The Microsoft Azure[10] environment is secured using the Federal Risk and Authorization Management Program (FedRAMP)[11] framework in a commercial high environment. The entity manages the encryption keys within the environment using a "customer lockbox" solution.

Scope

Scope of the exercise included:

- CIP-004-6 R1 Part 1.1, R2 (all Parts)
- CIP-004-6 R4 Parts 4.1, 4.4, R5 Parts 5.1, 5.3
- CIP-011-2 R1 (all Parts)

Experience Gained Summary

Further detailed below, is a summary list of the key experiences from this exercise.

1. CSP documentation was found valuable by the ERO Enterprise to help understand the cloud environment and to supplement the responsible entity's compliance documentation.
2. As a first of a kind, proof of concept, CSP engagement was essential for the development of RSAW narratives, documentation of environment and security controls, data request responses, etc. (This should not be expected nor needed for regular CMEP engagements.)
3. The responsible entity, ERO Enterprise, and the CSP all use different terminology to describe certain functionality and environments. The responsible entity needs to take extra care to make sure the CSP understands what certain terms mean in the CIP context.
    a. For example, logs produced from the cloud analytics may not look familiar to an auditor, necessitating extra explanation, highlighting, and justification.
    b. Another example is that the CSP may refer to backups as an application rather than a function.
4. Expect a deep dive on the following items:
    a. Methods used to protect BCSI in storage (at rest), in transit, and use.
    b. Encryption key management.
    c. Access control, particularly as it relates to CSP personnel.
    d. Active Directory (AD), including updating and synchronization.
    e. Security control considerations not called out by the CIP Standards (e.g. data sovereignty, services, etc.).
    f. How unauthorized access to BCSI is prevented after cloud services are terminated.
    g. Any CSP certifications that are relevant to the controls/protections being applied to secure the responsible entity's BCSI, including how those controls/protections are monitored, audited, etc.

[10] https://azure.microsoft.com/en-us/

[11] https://www.fedramp.gov/program-basics/

5. It is recommended that the responsible entity update their information protection program (CIP-011 R1.2), cyber security awareness (CIP-004 R1), and CIP training (CIP-004 R2) materials to address nuances specific to cloud services/environment
6. A schematic or compilation of the environment needed for the auditor to understand the environment.
7. These topics need further exploration with the ERO Enterprise to come to a conclusion:
    a. Whether use of data for computing is the same as use of BCSI (per CIP-011-2 R1.2).
        i. Note: page three of the approved Reliability and Security Technical Committee (RSTC) *"Security Guideline: Primer for Cloud Solutions and Encrypting BCSI"* on this topic it states, "Data in use refers to data that is being used or modified by an end-user."
    b. Whether documentation related to any relevant CSP certification and associated controls be utilized to provide direct evidence of compliance with the applicable NERC CIP requirements.

Preparation for Tabletop Exercise

1. The process document in Appendix A provides for preparation timelines and tasks. Early communication with the CSP is critical for establishing and ensuring objectives are understood from the beginning.
2. Consider using a test environment with test, draft, or example data to minimize any potential compliance issues. The responsible entity, ERO Enterprise, and CSP should evaluate and assess all relevant aspects and have complete comfort to look at any aspect of the test environment. All evidence provided should be marked as draft, unofficial, example, etc. if based on actual compliance evidence.
3. The test environment should have all controls in place, including monitoring, logging, and policies that identify issues and prevent misconfiguration.
4. If using a copy of production information, recommend obfuscating/masking data such that no sensitive information is disclosed.
5. Using test documents based on operational documents, such as draft versions of policies, plans, and procedures is useful because it makes adoption of changes (if needed) easier to operational documents.
6. Scheduling ERO Enterprise and CSP resources may be challenging — schedule ahead of time.
7. Prepare Reliability Standard Audit Worksheets (RSAWs) for the requirements relevant to the tabletop exercise only. This exercise did not utilize the *CIP Evidence Request Tool* (ERT).[12] Use of the ERT may be a consideration for future exercises.
8. When preparing RSAWs, share them with the CSP early on and work to add their information that may be relevant to the narrative.
9. Preparation of file sharing was critical. Training was performed on the tools for the external (ERO Enterprise/CSP) participants for the file access part of the exercise.
10. Internal WAPA review of the submitted documentation was done as if for a mock or actual audit. This prevented low-quality evidence from being submitted.
11. Following the preparation steps in Appendix A assured the exercise itself took only about four hours.
12. Non-Disclosure agreements (NDAs) were signed where necessary — do not leave out this important step. Some CSPs may need this to proceed with the exercise.

[12] https://www.nerc.com/pa/comp/CAOneStopShop/CIP%20Evidence%20Request%20Tool%20v7.xlsx

13. ERO Enterprise participants should pick a lead for questions ahead of the exercise. This can be handled on the pre-meeting seven days in advance according to Appendix A of the process document.
14. Be prepared to answer both compliance questions as well as risk-based questions you may have to answer for a self-report with a risk engineer.

Reliability Standard Audit Worksheets (RSAWs)

1. Generally, narratives were limited to relevance to the tabletop. An overview of the responsible entity's overall access management program was included since it also manages access to BCSI.
2. Given this is the first exercise using this process, the CSP also provided narratives and evidence as to what they do for access control and protection of data for the underlay of the cloud environment. Feedback from the ERO Enterprise indicated this was useful information for understanding but wasn't central to their evaluation. The recommendation is to consider including CSP documentation separately listed out by requirement unless it is directly applicable to answering the question in the RSAW.
3. The responsible entity used the regional-specific version of the RSAW, but this is no longer required.
4. Responsible entity and CSP narratives were separate in the RSAW. For example:
    a. **Entity Response**

       [Entity narrative]

       CSP Response

       [CSP narrative]

    b. This keeps editing to a minimum and ensures the ERO Enterprise clearly understand which party is providing the narrative.
5. The responsible entity does not edit any of the CSP narratives or evidence. Both are provided as-is. This prevents versioning problems and makes overall management of the RSAW preparation easier.

Roles and Responsibilities

1. The responsible entity led the process for organizing the implementing the tabletop exercise. A single point of contact should be established to manage tasks and be a communication hub. This also include after-action reports, follow-ups, and closing out the activity.
2. Use the teams table (Table 1) in the *BCSI in the Cloud TTX Generic Process Template* document to assign roles and responsibilities. The responsible entity will also need to assign internal roles and responsibilities as they would in a regular audit and ensure the appropriate departments are participating. Internal departments to consider beyond compliance are process owners, cloud implementation team, system administrators, administrative support (for notetaking and data requests), cyber security, and the IT compliance team.
3. Ensure the CSP stays engaged in the process. This was successful in this exercise and the CSP was able to clarify certain aspects about the environment, contract, and processes. The CSP may need to learn how a NERC audit is conducted

Evidence

General Evidence Takeaways

1. Where possible, the Registered Entity's identification of the relevant Standard and Requirement is indicated at the beginning of each heading.

2. All evidence was labeled via watermark as draft, example, or other label indicating it was for the exercise. Information potentially classified as BCSI was labeled as BCSI as well. All evidence was treated as BCSI regardless of labelling.
3. The responsible entity used evidence it determined relevant to the cloud, such as example reports of access authorizations to the environment.
4. All documents were highlighted to show the entities controls implemented relevant to their SaaS environment to minimize the ERO Enterprise searching the documents. (Evidence Formatting)

Detail of Evidence Provided and Associated Discussion:

1. Access Control Program Documentation
2. Cloud Service(s) Procurement Documentation: The ERO enterprise will read the contracts provided. Ensure relevant contract sections are highlighted. Referenced documents in the contract should also be provided and highlighted, e.g. a reference to a subscriber agreement. Below are the specific documents provided for this exercise:
    a. Responsible entity procurement agreement from the responsible entity showing what Azure product was purchased and shows the executed procurement (e.g. dated signatures). This was examined to ensure the contract was properly executed meeting entity/vendor legal requirements and when it became effective.
    b. This link describes the different contract types and terms listed below.
        i. Microsoft Online Services DPA (Data Protection Addendum)
        ii. Microsoft Online subscription agreement
        iii. Microsoft Online Services Terms
3. CIP-004-6 R4-R5: Expect detailed questions about logical access control into the environment, for example:
    a. How the responsible entity controls access, including timely removal of access. This will include a technical discussion if directory services are used, and what happens if certain parts of the access control system fail. Evidence from the technical system will need to be provided (e.g. system-generated logs).
        i. Recommend having an example showing how the environment is isolated to allow only trusted networks.
    b. Expect a thorough examination of how the CSP controls access to the responsible entity tenant overlay and data (customer data), including process, procedures, and contract requirements. Evidence may be requested, so know how to address that. Responsible entities should perform prior preparation with the CSP. For this exercise, the CSP provided procedures and contract language about how customer data is protected from CSP system and application administrators access unless specifically authorized by the customer, and only for a fixed period of time. The CSP procedures should address technical controls to prevent unauthorized access.
        i. This examination includes understanding how access is controlled between tenants, subscriptions, and other partitions found in the cloud environment.
    c. The ERO Enterprise asked for a list of services authorized into the cloud environment in order to understand the different applications and/or services that may have access to the environment. For this exercise, the test environment was isolated in that it did not have a network share, server, or any other delivery system in front of it. The CSP may need certain services for the environment itself to function,

namely for security monitoring, logging, and analytics. Ensure these are included and how changes to those services are controlled. Are they authorized by the responsible entity?

d. Be prepared to show that the list of responsible entity authorized users matches the list of cloud environment authorized users.

   i. The responsible entity should also ensure a subject matter expert can demonstrate user roles to show the users identity flows from the directory services (e.g. AD, OpenLDAP), if used. If single sign-on (SSO) is used, prepare for a technical discussion about policies and procedures on how it is to be used from a responsible entity user standpoint.

   ii. Prepare for a discussion of management groups and how those work to ensure the principle of least-permission.

e. Ensure that all administrative accounts needed to manage the cloud environment itself are included in the access control program, including shared accounts and those that exist only on the CSP side.

f. In this exercise, the responsible entity had detailed discussions showing what happens when a user is authorized for cloud access in the responsible entity's access control system and how that information passes to the cloud environment. The responsible entity worked with the ERO Enterprise to identify adequate evidence to show process either succeeding or failing. The reason for this discussion was to show how a gap between the cloud access control and responsible entity access control systems is minimized for access granting and removal.

4. CIP-004-6 R4-R5 and CIP-011-2 R1.2 (Evidence presentation): Evidence in the Azure environment consisted of a set of pre-configured policy templates that set certain monitoring, logging, access controls, and replication settings. A suggested improvement is to have an Excel report showing all the detailed settings of the environment. The policy templates were also necessary to show compliance with the policies via the available tools and dynamic compliance reports.

   a. Most of this evidence for the exercise was screenshots of settings from web pages. The ERO Enterprise participants indicated this was not their preferred method of presenting evidence artifacts.

   b. Expect to show that the policy is specifically applied to the test environment though a demonstration, screenshot, report, or log.

5. Cloud Security Model and Certification(s): If using a CSP environment that is covered by a certification (in this case FedRAMP), expect to discuss how the certification relates to the applicable CIP requirements, whether there are any 3rd party verification of those associated controls, and how the responsible entity maintains awareness of the certification status (including any findings/mitigations from a 3rd party audit). The objective is to ensure the responsible entity:

   a. understands each party's responsibilities under the shared responsibility model,

   b. has implemented what it is responsible for under that shared responsibility model, and

   c. knows how to reassess its security posture if/when the certification is revoked or there are findings from 3rd party audits.

      i. Also be prepared to provide assurance the environment has the stated certification. This can be done online or with provided reports from the CSP.

6. CIP-011-2 R1.2: Be ready for a deep technical discussion of methods used to ensure the confidentiality of data-at-rest (i.e. encryption). Be able to explain how the encryption works and who controls the keys. In this exercise, the responsible entity controls the keys, and demonstrated the tool used to rotate the keys. The responsible entity also showed logs produced when the keys are rotated, created, or removed. The CSP may need to be involved in this conversation depending on the technical process.

   a. Be prepared to discuss the scope the keys are applied to, e.g. the entire subscription, a certain tenant or environment.

7. CIP-011-2 R1.2: A technical discussion of data transmission (in-transit) is likely. Ensure an SME can show what version of encryption is being used for data in transit, e.g. TLS v1.2.

8. CIP-011-2 R1.2: For this exercise, the responsible entity had a requirement in their information protection program that all data be kept within the continental United States. As a result, the ERO Enterprise asked how geo-replication of the test environment (replication between different geographical locations) was performed. Evidence included a list of the policies that prevent selection of replication locations outside the continental United States, including the actual technical policy definition and a screenshot of the replication set-up process showing that a violation of the policy will fail to deploy.

9. CIP-011 R1.2: Be prepared to demonstrate how unauthorized access to BCSI is explicitly prevented when a CSP subscription is terminated. Demonstrating the ability to delete BCSI in the environment, drop all encryption keys, or deleting the container itself would likely be required to ensure access to BCSI following termination of CSP subscription has been precluded.

   a. Recommendation is to ensure that encryption keys are dropped and the BCSI container is deleted prior to disassociation, along with the documentation the deletion was completed successfully.

   b. For this exercise, the CSP also keeps backups 90 days after subscription termination. Be prepared to discuss assurance the CSP cannot access the content of the backup copy.

   c. Responsible entity also provided Microsoft procedures for canceling the Azure subscription, data management, and data access management. These were available online from Microsoft. Have similar documents available from your CSP.

10. Draft list of identified BCSI repositories within the Azure environment (CIP-011-2 R1.1)

11. Draft registered entity-specific Information Classification Policy and Procedures document that includes: (CIP-011-2 R1)

   a. Requirement to geo-replicate and data residency only in the continental USA

   b. Definition of Automated Information Processing System, a defined term used in WAPA-specific policies, modified to include the CSPs approved by the responsible entity.

   c. Physical storage procedure requires FedRAMP CSP environments of medium or higher (as the responsible entity is a federal agency).

   d. Requirement for electronic storage that keys must be controlled by the responsible entity in a cloud environment for this particular tabletop scenario, with annual key rotation at a minimum and on an as-needed basis.

12. A draft document describing the responsible entity's overall cybersecurity awareness program, (CIP-004-6 R1 and R2 Part 2.1.5). For the exercise, the responsible entity supplied information to show awareness performed for handling of BCSI information within a cloud environment.

   a. Includes examples of various cyber-awareness publications that address cloud-related cybersecurity issues

13. Example of changes to the responsible entity's annual cyber security training slides showing cloud-specific information (CIP-004-6 R2):

   a. Definition of cloud computing

   b. A suggestion from the ERO Enterprise was to ensure to point out that a cloud environment is external to the responsible entity.

c. Slide about requirements for local administrator accounts updated to include cloud management accounts

d. Updated list of approved systems designated for storing BCSI includes Microsoft Azure. This includes an updated description of access-control system roles that include Microsoft Azure.

e. Note there is no requirement to specifically address cloud-specific BCSI handling procedures. Given this was the first iteration of this exercise; draft training/awareness was included in the scope for completeness. Other exercises may not find this is necessary to put this in scope.

14. WAPA CIP Exceptional Circumstances document updated to include critical connectivity to or availability of cloud-based services containing BCSI repositories under the imminent failure of hardware, software, or equipment section (CIP-004-6 R2.2, R4.1).

FedRAMP Certification for Public Agency Cloud Environments

Extensive conversations took place about FedRAMP, which is required for the responsible entity as a public agency, and how it provides assurance of the security posture for the CSP's underlay infrastructure. The auditors want to know how the responsible entity controls access into their tenant overlay and to BCSI within that environment (CIP-004-6 R4, R5 and CIP-011-2 R1.2).

This is a new concept for CMEP activities and no specific conclusions were reached during the exercise as to the extent that FedRAMP certification could be used to provide direct evidence of compliance. The responsible entity is planning to continue that discussion with the ERO Enterprise and CSP.

Chapter 5: Process

1. The overall tabletop process was considered a success by the participants. Suggested improvements:
    a. Begin with the CIP-004 access control program discussion. This allows the ERO Enterprise to understand the responsible entity's access control program.

    b. Preparation effort is what kept the tabletop exercise to the planned four hours. Preparation steps are incorporated into the latest version of the process document. Keeping to the established timetable also assured maximum time efficiency, which is an objective of the tabletop process.

    c. The responsible entity needs to keep in contact with the ERO Enterprise participants and the CSP, as after-action activities such as data requests may require some added communication.

    d. Have a note taker present as well as someone to handle data requests. Also, encourage all participants to take their own notes, with the intention of sharing them with the team. This captures perspectives from all participants.

    e. Make sure to include introductions at the beginning of the exercise. This helped verbal communication immensely. On WebEx, also make sure, if possible, that participant's names and organization are shown, e.g. John Smith, ABC Utility.

    f. The ERO Enterprise needed to have offline conversations after the exercise to determine what additional questions to ask, and to determine generally how the evidence might meet compliance requirements and make recommendations on evidence clarity and quality.

Chapter 6: Other Key Takeaways

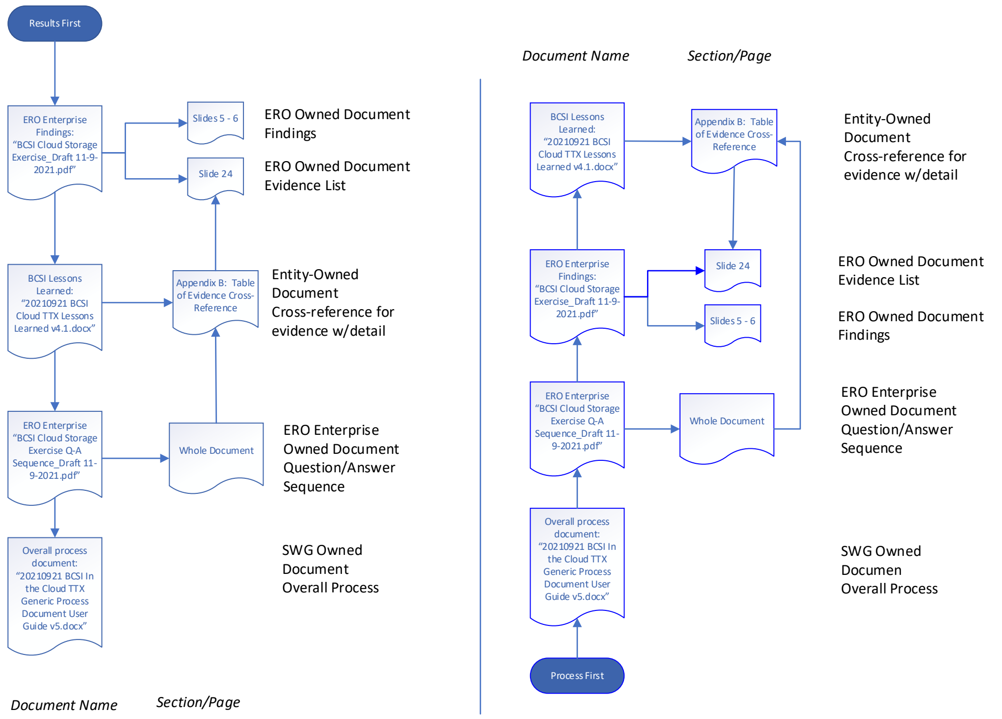
1. As the responsible entity, be able to explain why the CSP is trusted by your organization, and how you maintain that trust. Examples include certifications and risk evaluation during the procurement process, etc. Some organizations have a formal authority to operate process that could be used to answer these questions.

2. Do not assume the auditor has expert experience for every aspect of cloud computing. The tabletop exercise value is to educate the ERO Enterprise and CSP as well as the responsible entity. Extra effort is needed to make sure that participants understand the questions being asked and understand the answers being given. If not, take the time to get that understanding while the participants are assembled.

3. This initial set of deliverables took longer than planned to assemble, review, and release. A future improvement to the process should be to put timeline objectives for the after-action activities to decrease this part of the process.

Appendix A: Deliverable Document Relationships

Use this diagram to follow the relationship between the documents of the deliverable package. The arrows indicate how to read the documents. The approach on the left is looking with the results first. The approach on the right is looking at the process first.



Results First
ERO Enterprise Findings: "BCSI Cloud Storage Exercise_Draft 11-9-2021.pdf"
Slides 5 - 6
ERO Owned Document Findings
Slide 24
ERO Owned Document Evidence List
BCSI Lessons Learned: "20210921 BCSI Cloud TTX Lessons Learned v4.1.docx"
Appendix B: Table of Evidence Cross-Reference
Entity-Owned Document Cross-reference for evidence w/detail
ERO Enterprise "BCSI Cloud Storage Exercise Q-A Sequence_Draft 11-9-2021.pdf"
Whole Document
ERO Enterprise Owned Document Question/Answer Sequence
Overall process document: "20210921 BCSI In the Cloud TTX Generic Process Document User Guide v5.docx"
SWG Owned Document Overall Process
Document Name
Section/Page
Document Name
Section/Page
BCSI Lessons Learned: "20210921 BCSI Cloud TTX Lessons Learned v4.1.docx"
Appendix B: Table of Evidence Cross-Reference
Entity-Owned Document Cross-reference for evidence w/detail
ERO Enterprise Findings: "BCSI Cloud Storage Exercise_Draft 11-9-2021.pdf"
Slide 24
ERO Owned Document Evidence List
Slides 5 - 6
ERO Owned Document Findings
ERO Enterprise "BCSI Cloud Storage Exercise Q-A Sequence_Draft 11-9-2021.pdf"
Whole Document
ERO Enterprise Owned Document Question/Answer Sequence
Overall process document: "20210921 BCSI In the Cloud TTX Generic Process Document User Guide v5.docx"
SWG Owned Documen Overall Process
Process First

Figure A.1: Deliverable Documents Relationship Flowchart

Appendix B: Evidence Cross-Reference Table

This table maps documents to the evidence list maintained by the ERO Enterprise team. Not used, means the data was asked for, but not used beyond review by the ERO Enterprise. It is a placeholder to keep the file references consistent.

Table A.1: Evidence Cross-Reference

Reference Number	Name	Standard	Requirement	Description
1	CSP Business Agreement	N/A	N/A	Business Agreement. Included in CIP-004-6 R1.1 as part of overall security model
2	Isolation Choices	CIP-004-6	R4-R5	Tenant isolation and access control between tenants
3	HTTPS	CIP-011-2	R1.2	Shows HTTPS connectivity and encryption qualities (data in transit)
4	Customer Managed Keys	CIP-004-6	R4-R5	Screenshot showing settings for customer-managed encryption keys
5	Not Used	N/A	N/A	Not Used
6	Access solution	CIP-004-6	R4-R5	Describes Microsoft just-in-time access control process in context of Microsoft support staff having access to the tenant
7	Not Used	N/A	N/A	Not Used
8	Business Agreement Order	N/A	N/A	Purchase Order showing purchase of cloud environment was executed (a valid agreement)
9	Regional Entity RFI-1	CIP-004-6 / CIP-011-2		Regional Entity response to ERO Enterprise RFI-1. Responses include topics relevant to both CIP-004 and CIP-011, and covered both audit and self-report scenarios
10	Network Isolation Example	CIP-004-6	R4	Screenshot of settings demonstrating customer environment is containerized and isolated from other tenant environments.
11	TLS Policy 1	CIP-011-2	R1.2	Screenshot of technical policy forcing TLS version for data in transit
12	TLS Policy Shown	CIP-011-2	R1.2	Screenshot showing technical policy setting for TLS meets automated compliance check
13	Location Policy Detail	CIP-011-2	R1.2	Screenshot showing technical policy setting demonstrating that data centers that support this Azure service are known and controlled by the entity.
14	Geo-Replication Policy	CIP-011-2	R1.2	Screenshot showing technical policy controlling geo-replication is enabled and active. Used with #13 to demonstrate that data centers that support this Azure service are known and controlled by the entity.
15	Encryption Fundamentals	CIP-011-2	R1.2	Document from Microsoft used as an extra reference to further explain how Microsoft accomplishes encryption for data at rest.

Table A.1: Evidence Cross-Reference				
Reference Number	Name	Standard	Requirement	Description
16	Key Vault Config	CIP-004-6	R4-R5	Document from Microsoft describing how the Key Vault product securely stores secrets and keys
17	AD Config	CIP-004-6	R4-R5	Entity document with details on how AD is configured via federation services
18	AD Config 2	CIP-004-6	R4-R5	Screenshots showing AD Federated services are enabled, AD account synchronized from entity on-prem domain controllers only, and AD groups replicated to Azure from entity only. Also some technical explanation of how removals from the entity on-prem AD controllers would work.
19	AD Sync	CIP-004-6	R4-R5	Screenshot showing details of AD sync status and AD federation settings
20	Subscription Cancellation	CIP-004-6	R4, R5.3	Microsoft document with procedure for canceling the subscription, used to understand how CSP access to BCSI is prevented by the entity information protection program following termination of services.
21	Trusted Services	CIP-004-6	R4, R5.3	Microsoft procedure for configuration of storage firewalls and virtual networks, used to understand how CSP access to BCSI is prevented by the entity information protection program following termination of services.
22	Data Management	CIP-004-6	R4, R5.3	Microsoft document explaining data retention and data deletion on physical storage devices, used to understand how CSP access to BCSI is prevented by the entity information protection program following termination of services.
23	Data Access Management	CIP-004-6	R4, R5.3	Microsoft document describing who can access entity data and on what terms. Includes descriptions of operational processes governing customer data, how access is limited, and how subprocessor access to customer data is managed. Used to understand how CSP access to BCSI is prevented by the entity information protection program following termination of services.
24	RE RFI-2	CIP-004-6 / CIP-011-2	Multiple	Entity response to ERO Enterprise RFI-2. Responses include topics relevant to both CIP-004 and CIP-011, and covered both audit and self-report scenarios.

Table A.1: Evidence Cross-Reference				
Reference Number	**Name**	**Standard**	**Requirement**	**Description**
25	BCSI designated storage memo	CIP-004-6	R4.4	Entity document identifying the designated storage location for BCSI (included cloud location).
26	Create Resource Fail	CIP-011-2	R1.2	Screenshot showing a create resource failure resulting from a geo-location policy enforcement.

Appendix C: Version History

Document Version History

Version History		
Version	**Date**	**Description**
0.1	August 8, 2022	Original draft version
1.0	March 22, 2023	Approved by the Reliability and Security Technical Committee

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

BCSI in the Cloud Tabletop Exercise Generic Process Template

Version 5.3: March 22, 2023

Overview

This document provides samples and recommendations for entities that wish to conduct a tabletop exercise that simulates the use of a cloud-based solution for protecting Bulk Electric System (BES) Cyber System Information (BCSI). The items throughout this document that are shown in red indicate actions or information that the entity will need to perform, develop, or decide.

The purpose of this exercise is to review and evaluate cloud-based technologies and the ability of an entity to demonstrate compliance with NERC Critical Infrastructure Protection (CIP) requirements. The scope includes a study of the features and specifications of cloud technologies and potential services that may correlate to applicable requirements of the CIP Reliability Standards. The outcome of this effort may include the development of implementation guidance, lessons learned, NERC Standard Authorization Requests, or industry whitepapers.

Assessment Scope

This exercise is limited solely to a review of an entity's approach to using cloud technologies to transfer, store, and use NERC defined BCSI and does not review or consider cloud-based BES Cyber Systems (BCS) operations. Participating Registered Entities may want to consider a cloud provider with which they have an existing relationship or contract, or include a cloud service or cloud service provider in which they may be interested for future services.

The Scenario Being Tested

- Responsible Entity: [Responsible Entity Name]
- Cloud Service Provider (CSP): [CSP]
- Cloud Security Framework: [Federal Risk and Authorization Management Program (FedRAMP), National Institute of Standards and Technology (NIST), another framework]
- Encryption: [Customer Managed | CSP Managed | Other (describe)]
- CSP Service: [Infrastructure as a Service (IaaS), Performance and Energy-Aware Scheduling (PEAS), Software as a Service (SaaS), etc.]
- Object(s): [Describe the objects being evaluated, e.g., file share, storage infrastructure, etc.]
- Method: Remote document review and interview with sample Reliability Standard Audit Worksheets (RSAWs) and sample evidence

- Third Party Audit Organization (3PAO)[1] (if applicable): [3PAO]
- Compliance Scope [2]
  - CIP-004-6 R1 P1.1, R2 P2.1 – 2.3, R4 P4.1, 4.4, R5 P5.1 – 5.3
  - CIP-011-2 R1 P1.1 – 1.2, R2 P2.1 – 2.2

NOTE: If a participating Registered Entity is currently storing and/or utilizing BCSI in the cloud, and they choose to include the analysis of such in this tabletop exercise, no waiver of compliance will be offered/available.

Team

Table 1: Tabletop Team Members

Role	Description	Individuals
Vendor(s)	• Participate in Tabletop exercise to identify controls, evidence, etc.	[Names, Company]
Auditor(s)	• Provide subject matter expertise from auditor and CMEP perspective	[Names, Company]
Security Working Group (SWG) Member(s)	• Provide subject matter expertise from Responsible Entity perspective; • Provide overall direction and leadership to the Tabletop; • Schedule meetings; • Escalate key issues and recommendations on behalf of Tabletop Team.	[Names, Company]
NERC/Electric Reliability Organization (ERO) Rep	• Provide subject matter expertise; • Support resolution of key issues and recommendations escalated for the Tabletop Team.	[Names, Company]

[1] Third Party Assessment Organizations (3PAOs) play a critical role in the authorization process by assessing the security of a Cloud Service Offering. As independent third parties, they perform initial and periodic assessments of cloud systems based on federal security requirements. (https://www.fedramp.gov/assessors/#:~:text=%C2%AE,based%20on%20federal%20security%20requirements.)

[2] The CIP Reliability Standards referenced in this document cite the currently effective versions as of the date of publication. Users should verify that they are using currently effective standards and requirements.

FERC Rep(s)	• Provide subject matter expertise from the FERC perspective	[Names, Company]
[Responsible Entity] Rep(s)	• Provide subject matter expertise for implementation • Solicit support from their cloud service providers; • Work with vendors to identify controls, evidence, etc.; Attend meetings; • Escalate issues if necessary.	[Names, Company]

Objectives

- Provide a framework to develop and improve an assessment process for BCSI in a cloud environment.
- Review evidence to demonstrate compliance with the CIP Reliability Standards based on controls implemented by the Responsible Entity and/or [Cloud Security Framework] certification processes. Determine if evidence and controls are sufficient to demonstrate CIP Compliance as they pertain to BCSI requirements in CIP-004-6 and CIP-011-2 specifically.
- Provide Responsible Entities and their CSPs with guidance and information regarding the controls and evidence that are necessary to demonstrate compliance with the CIP Reliability Standards.
- Provide experiences about the assessment approach and the way evidence provided for CIP interrelates with NIST[3]-based controls as governed by [Cloud Security Framework].
- Provide experiences about the tabletop process to make future assessments with different scenarios valuable to all stakeholders.
- Note that several tabletop exercises using different scenarios may need to be completed to offer quality guidance.

Phase 1

CIP-011-2 — Cyber Security — Information Protection R1

1. Confirm the Responsible Entity has a method to classify Method(s) to identify information that meets the definition of BCSI, including identifying cloud-based repositories.
2. Determine contract-based responsibilities for information classification between [CSP] and [Responsible Entity].

[3] https://www.nist.gov/

3. Determine, along with the Responsible Entity's processes and procedures, if existing types of certifications for [Cloud Security Framework] may also be utilized to demonstrate sufficient vendor controls, e.g., NIST controls listing with [Cloud Security Framework] evidence of controls testing for the following:
    a. Procedure(s) for protecting and securely handling BCSI, including storage, transit, and use.
4. Determine and document identified deficiencies

Follow-Up Activities

1. Identify next steps including potential industry deliverables/reporting, additional phases or efforts, and Reliability Standards revision recommendations
2. Create deliverables such as experiences, if possible, or, if not possible, implementation guidance, if such development of such guidance is possible
3. Develop and implement a communication plan for resulting deliverables and/or provide Reliability Standards revision recommendations to the Standards Committee
4. Develop planning team for additional phases

Phase 2

CIP-004-6 – Access Management Program - Granting and Revoking Electronic and Physical Access to BCSI.

1. Identify the requirements and expectations for Access Management and Access Revocation (Refer to Reliability Standard) and the set of data to be collected from both [CSP Service] and [Responsible Entity] access authorization and access control systems.
2. Identify the evidence required to prove compliance
3. Identify applicable technical controls from both [CSP] and [Responsible Entity] can apply
4. Determine the process and effort involved for producing evidence between the [Responsible Entity] and [CSP] for both the access control process and controls evidence

Follow-Up Activities

1. Create experiences, if possible, or, if not possible, implementation guidance, if such development of such guidance is possible
2. Develop a communication plan for resulting deliverables

Phase 3

Assessment of Implemented Controls between [CSP] and [Responsible Entity] and Approaches to be Considered: Encryption and [Cloud Security Framework] Framework)

1. Determine if existing types of certifications for [Cloud Security Framework] may be utilized to demonstrate sufficient vendor controls, e.g., NIST controls listing with [Cloud Security Framework] evidence of controls testing.
2. Determine how data encryption and key management responsibilities have an effect on demonstrating compliance.
3. Determine if the [3PAO] report provides sufficient evidence to demonstrate BCSI requirements.
4. Map
    a. Outcomes from [CSP Service] to the identified requirements and controls, where possible. This can be accomplished using the applicable RSAWs.
    b. Methods, approaches, and policies that were effective in implementing the technical controls of the CIP requirements. These can be addressed in the RSAWs.
    c. Issues that were encountered and how they were resolved or if they were not resolved, e.g., a deficiency was identified.
    d. Where outcomes differed from expectations (i.e., easier or more difficult than expected).
    e. CIP requirements that posed particularly difficult challenges.
    f. What would have been done differently with the benefit of hindsight?
    g. Business or supply chain challenges that were encountered and how they were addressed.
    h. Determine and document identified deficiencies

Follow-Up Activities

1. Identify next steps including potential industry deliverables/reporting, additional phases or efforts, and Reliability Standards revision recommendations
2. Create deliverables such as experiences, if possible, or, if not possible, implementation guidance, if such development of such guidance is possible
3. Develop and implement a communication plan for resulting deliverables and/or provide Reliability Standards revision recommendations to the Standards Committee
4. Develop planning team for additional phases

See Appendix D for a list of deliverables to be produced and associated ownership responsibilities.

Appendix A: Preparation Activities for [Responsible Entity]

This section is a basic checklist of activities the responsible entity should perform to ensure an effective exercise. Dates are based on experiences from the previous exercises.

Tools and Technology

1. This tabletop exercise is envisioned to be a virtual activity. Tools are provided by the organizing responsible entity. Potential tools include:
   a. A secure file-transfer server that allows file viewing but not downloading by external participants. Recommendation is to ensure everyone knows how to navigate the secure file server and view documents in advance of the tabletop activity.
   b. A conferencing application (WebEx, Zoom, Teams, etc.) for pre-meetings and the tabletop itself. Video should be enabled when practical. Sharing of documents or live demonstrations on the screen can be performed when required.
   c. A telephone conference bridge for a back-up.
   d. A scheduling website for determining the best time to schedule the activity

60 – 90 Days in Advance

1. Update the *BCSI in the Cloud Tabletop Exercise Generic Process Template* (this document) with the correct information and communicate it to the CSP. Ensure the CSP is aligned with the objectives and scope of the tabletop plan.
2. Set up test environment working with the CSP. Determine:
   a. Type of object to use (e.g., file share, generic information store, etc.)
   b. Controls that are implemented around the object
   c. Dashboard reports
   d. Activity logs and associated reports
   e. Relevant CSP documentation about the controls, dashboard, reports, and automation supporting the environment. These can include CSP-provided documentation if directly relevant.

45 Days in Advance

3. Determine date, time, and duration of the activity
   a. *Recommendation: Use a scheduling tool such as Doodle*
4. Recruit exercise team members as outlined in this document
   a. Contact SWG chair to send out a call for volunteers or use direct contact with your Regional Reliability Organization (RRO), ERO representatives

   b. *Recommendation: Ensure you have full contact information for each exercise team member, especially mobile phone*

5. Create a schedule for involved participants and groups (internal and external)
6. Begin assessment of RSAWs and evidence to find gaps (policies, processes, and procedures)
7. Ensure remote tools are configured, scheduled, etc. Tools include secure file transfer (Box, Kiteworks, etc.) and remote meeting (Zoom, Webex, etc.).
   a. Set file transfer tool to allow for viewing but not downloading documentation

30 Days in Advance

8. First internal draft of RSAWs completed, including narratives and evidence
9. Confirm schedules for participants
10. Ensure non-disclosure agreements are in place for the ERO, RRO, and CSP
11. Ensure backup plans are in place in the event of network, virtual private network (VPN), or tool failure.
    a. *Recommendation: Have a phone conference bridge set up to fall back to.*
12. Pre-tabletop virtual meeting scheduled for external exercise participants (e.g., vendor, ERO, RRO representatives). See **Appendix B** for sample agenda. Meeting should be scheduled approximately 7 days in advance of the tabletop.
13. Advise internal management of the tabletop activity.
    a. *Recommendation: Schedule a senior leader to give a short welcome message to the exercise team at the start of the tabletop.*

14 Days in Advance

14. Final review of RSAWs, narratives, and evidence
    a. Ensure internal stakeholders are aware of the documentation and are prepared to be asked questions
15. Final availability check for exercise team members

7 Days in Advance

16. RSAWs, narratives, evidence, team members, and CSP environment are set and will not be changed unless there is a technical issue.
17. Files uploaded to file transfer tool so external parties can begin assessment
18. Facilitate pre-tabletop virtual meeting
19. Ensure all team members can access the documentation on the file transfer site (CRITICAL)

1 Day in Advance

20. Reach out to external team members to ensure they are set and there are no last-minute problems or issues
21. Email out the backup plans in case of tool or network failure to all team members. (See Appendix C.)

Day of Tabletop

22. Allow at least two hours of time prior to the activities for last-minute troubleshooting and questions
23. Start the remote meeting tool at least 30 minutes in advance.
24. At the start of the tabletop, schedule in 15 minutes to go over the agenda for the day and introduce team members.

Appendix B: Agenda for Pre-Tabletop Meeting

1. Review the general schedule for the exercise
2. Review the objectives and expectations of the exercise
3. Discuss confidentiality for [Responsible Entity] and [CSP]-specific information
4. Ensure everyone can access the information via the file transfer tool
5. Discuss and decide the assessment team tools (e.g., blank RSAW)
6. Feedback desired from the audit team
7. Format and distribution of notes
8. Review of expected output from this exercise (e.g., experiences)
9. Post-tabletop activities review
10. Q&A for the assessment team

Appendix C: Example Backup Procedures in the Event of Network/Tool Failure

Table 1: Network/Tool Failure Backup Procedure Examples

Condition	Action – [Responsible Entity]	Action – Outside [Responsible Entity]	Resources Impacted	Workaround
[Responsible Entity] VPN Fails	Switch off VPN and rejoin WebEx	None	We will lose access to [CSP] portal and internal [Responsible Entity] file repository. Delay around 10 minutes while people get reconnected.	We have screenshots of the portal in the RSAW evidence. Meeting host has a local copy of the files in the repository that can be displayed on the meeting tool
Meeting host computer audio fails or is wonky	Switch to phone audio	Switch to phone audio	Delay of 5 minutes to get reconnected.	Switch to phone audio
Virtual meeting host has issues	Host will rejoin by phone or computer	None	Host should automatically fall back to another participant to keep the meeting up. No delay.	Alternate hosts will take over facilitating the exercise.
Participant is cut off because of freeze, reboot, ISP dies, etc.	Send meeting host a text at [xxx-xxx-xxxx]	Send host a text at [xxx-xxx-xxxx]	May have to pause until participant returns – will decide on the fly. Probably no delay.	Participant can call in via phone to the meeting.
Secure file transfer server fails/inaccessible	Host will call the appropriate help line	None	Critical impact as Kiteworks is the data repository for this exercise. Significant delay to get restored.	May have to reschedule the exercise if the delay is > 1 hour

Table 1: Network/Tool Failure Backup Procedure Examples

Condition	Action – [Responsible Entity]	Action – Outside [Responsible Entity]	Resources Impacted	Workaround
Meeting tool fails/inaccessible, total failure except for secure file transfer server	Call into the conference bridge.	Call into the conference bridge.	Loss of screen display, but voice will still work. Delay of probably 10 minutes.	Dial [yyy-yyy-yyyy]. When prompted, dial your conference code (zzzzz) and then hit the pound sign (#). If prompted for your name, say your name and then hit the pound (#) again. Text meeting host if you have issues joining.
100% technological failure	Host to send texts to all participants of the issue	None until contacted	No file transfer server, no conference bridge, no internet, no VPN	Reschedule tabletop

Appendix D: Deliverables Package

The following deliverables should be produced for experiences. There is an important division of ownership among the different deliverables:

1. Owner: Responsible Entity
    a. Updated technical reference document in NERC format
        i. Recommendations for producing evidence (e.g., cloud tools, reports, format, etc.)
        ii. Pitfalls or other areas of compliance or security risk identified during the exercise
        iii. Improvements to the process (preparation, timing, communication, etc.)
    b. RSAWs with generic types of evidence provided for the relevant requirements
    c. Non-public internal notes, other material used to create a public version (redacted) of the technical reference package
2. Owner: Cloud Service Provider
    a. CSP procedures, business agreements, product and service descriptions, and general cloud security model
    b. Ensure to communicate with the CSP to determine what appropriate information to put into the experiences or technical reference document
3. Owner: Security Working Group
    a. Updated process document considering feedback from the Responsible Entity
    b. Reviewed public version of technical reference package from the Responsible Entity
4. Owner: ERO Enterprise (NERC).
    a. List of possible risk areas as perceived by the ERO, CSP, or the responsible entity (includes compliance, cyber security, or other category) and potential mitigations.

Each owner is responsible for maintaining, reviewing, and editing its own portion of the technical reference package. This simplifies ongoing management. The final public version of the technical reference document should have web links to the other owners' documentation to make it easy to assemble the complete set of information.

Tips and Tricks

1. The after-action activities, such as the technical reference document and the associated deliverables package, should be reviewed by the ERO Enterprise, CSP, and internally by the responsible entity to minimize the chance of confidential information being released.
2. This tabletop exercise was envisioned to be a virtual activity. All tools were provided by the organizing Responsible Entity. tools used:
    a. A secure file-transfer server that allowed file viewing but not downloading by external participants.
        i. Verification of access and functionality was performed prior to the tabletop according to the process document **Appendix A**.
        ii. Auditing was turned on to monitor ERO Enterprise activity and validate proper functionality of login, access, etc.
    b. WebEx for pre-meetings and the tabletop itself. Video was enabled when practical. Sharing of documents or live demonstrations on the screen were performed when required.
    c. A telephone conference bridge for a back-up to the WebEx.
    d. Doodle.com for determining the best time to schedule the activity
    e. Training for the secure file server was performed and could be enhanced in the future.
        i. Recommendation is to ensure everyone knows how to navigate the secure file server and view documents.

Revision History

Version	Date	Who	Notes
1.0	1/30/2020	Martin	Initial version
2.0	6/1/2020	Sessions	New template, added Appendices, added recommendations from 5/21/2020 initial tabletop
3.0	3/17/2021	Sessions	Review and added Appendix D
4.0	9/21/2021	Sessions	Updated after SWG and ERO teams reviews
5.1	3/22/2023	RSTC	Approved
5.2	4/15/2023	Stephanie Lawrence Tom Hoffstetter	Admin review and cleanup
5.3	6/5/2023	Sessions	Final Updates

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-004-6 – Cyber Security – Personnel & Training

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		
R5	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			
R2			
P2.1			
P2.2			
P2.3			
R3			
P3.1			
P3.2			
P3.3			
P3.4			
P3.5			
R4			
P4.1			
P4.2			
P4.3			
P4.4			
R5			
P5.1			
P5.2			
P5.3			
P5.4			
P5.5			

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 implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [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-004-6Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R1 Part 1.1

CIP-004-6 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

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.

NOTE: RE elected to put general contract description in this section for the tabletop exercise because there was no other place to put it. This might not normally need to go here in an actual audit.

RE has an active subscription with Microsoft Azure. The conditions of the subscription agreement, including customer (RE) vs. Cloud Provider (Microsoft) responsibilities are outlined in [Online Subscription Document] and [Microsoft Online Document].

The Cloud Service Provider (CSP) does not have logical, physical access to RE High and Medium Impact BES Cyber Systems and associated EACMS, PACS and PCAs.

RE provides security awareness training to its employees and vendors at least once every calendar quarter to reinforce cyber security practices for personnel with authorized electronic access to cloud-based and on-premises resources.

RE reinforces Security Awareness as explained "RE Cyber Security Awareness Program Document", by providing one or more of the following:

- Quarterly email to all RE employees and contractors containing security awareness information
- Quarterly articles on RE internal web site

Examples of awareness are in the evidence file list below.

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-004-6, R1, Part 1.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which include security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.
	Verify the Responsible Entity has reinforced security awareness at least once each calendar quarter.
	Verify the security awareness reinforcement included: • reinforcement of cyber security practices, or • reinforcement of physical security practices associated with cyber security.
	Verify that security awareness was reinforced for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.
Note to Auditor: The Responsible Entity is not required to document that each quarter's reinforcement was received by each of its authorized personnel. Rather, the Responsible Entity is required to demonstrate that the security awareness reinforcement was communicated to its authorized personnel as a whole, not necessarily individually.	

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-6 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-6 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

R2 Part 2.1

CIP-004-6 Table R2 – Cyber Security Training Program			
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 with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

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.

The Cloud Service Provider (CSP) does not have logical, physical access to RE High and Medium Impact BES Cyber Systems and associated EACMS, PACS and PCAs.

The RE Cyber Security Awareness Program, "[Program Document]" addresses cyber security training topics required under requirement 2, part 2.1.5.

All RE employees are required to participate in cyber security training regardless of role, function or responsibilities as explained in "[Program Document]". The Critical Infrastructure Protection Training training can be found in the powerpoint presentation [Presentation] nd includes content on how to handle BCSI and it’s storage.

RE trains system administrators who design and manage a CSP environment. Training includes controls that are controls related to shared touch points in the Azure authorization boundary and any customer applications leveraging Azure infrastructure. [Link to Azure Operational Security best practices Document].

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
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

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

Compliance Assessment Approach Specific to CIP-004-6, R2, Part 2.1

This section to be completed by the Compliance Enforcement Authority

	Verify that the training program(s) collectively include content on the following: 1. Cyber security policies; 2. Physical access controls; 3. Electronic access controls; 4. The visitor control program; 5. Handling of BES Cyber System Information and its storage; 6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity’s incident response plan; 7. Recovery plans for BES Cyber Systems; 8. Response to Cyber Security Incidents; and 9. Cyber security risks associated with a BES Cyber System’s electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.
	Verify the Responsible Entity’s training program’s content is appropriate to individual roles, functions, or responsibilities.
Notes to Auditor:	

1. The training program(s) must collectively include all nine training elements.
2. It is not necessary that all nine training elements be included for the training of each role, function, or responsibility.
3. Each role, function, or responsibility must receive training on all appropriate training elements.

Auditor Notes:

R2 Part 2.2

CIP-004-6 Table R2 – Cyber Security Training Program			
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 with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.

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.

The Cloud Service Provider (CSP) does not have logical, physical access to RE High and Medium Impact BES Cyber Systems and associated EACMS, PACS and PCAs.

The RE access management program "[Program Document]" explains the onboarding workflow and modify access workflow. For both on-boarding or access modification activities, the workflow, supported in the RE Access Control System, checks to see if the individual is being granted access to CIP assets and, if true, requires the training validation and PRA date validation prior to initiating access authorization tasks. Section xxx discusses the processes for requiring completion of Cyber Security training.

RE during the audit period has not declared a CIP Exceptional Circumstance. In the event a condition occurs requiring RE to declare a CIP Exceptional Circumstance, RE follows guidance documented in "[Document]".

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**
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

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

Compliance Assessment Approach Specific to CIP-004-6, R2, Part 2.2

This section to be completed by the Compliance Enforcement Authority

	Verify all personnel completed the training specified in Part 2.1 prior to being granted authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.
	If the Responsible Entity has declared and responded to CIP Exceptional Circumstances, verify the Responsible Entity has adhered to the 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.	

Auditor Notes:

____

R2 Part 2.3

CIP-004-6 Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.3	High Impact BES Cyber Systems and their associated: • EACMS; and • PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

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.

The Cloud Service Provider (CSP) does not have logical, physical access to RE High and Medium Impact BES Cyber Systems and associated EACMS, PACS and PCAs.

The RE Cyber Security Awareness Program "[Program Document]" addresses R2 Part 2.3. "[Non-Completion Report]" is a sample report showing what employees have not completed the training. Follow-up actions to ensure completion include reminders sent to managers and supervisors prior to the mandatory completion date as shown in "[Example1]". If training is not completed within required timeframes, access is removed.

RE requires all employees to participate in its annual cyber security training program utilizing online training and testing program. [Program Document] discusses the processes for requiring completion of Cyber Security Training.

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
[redacted]					

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

Compliance Assessment Approach Specific to CIP-004-6, R2, Part 2.3

This section to be completed by the Compliance Enforcement Authority

	Verify all personnel with authorized electronic access or authorized unescorted physical access to applicable Cyber Assets completed the training specified in Part 2.1 at least once every 15 calendar months.

Auditor Notes:

R3 Supporting Evidence and Documentation

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-6 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-6 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

R3 Part 3.1

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
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 with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

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.

A PRA for information access is not required under CIP-004-6.

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-004-6, R3, Part 3.1

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that include a process to confirm identity.
	Verify a process to confirm identity was implemented for personnel with authorized electronic access and/or authorized unescorted physical access to Applicable Systems.

Auditor Notes:

R3 Part 3.2

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
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 with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1 current residence, regardless of duration; and 3.2.2 other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

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.

Please see response to P3.1.

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-004-6, R3, Part 3.2

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that include a process to perform a seven year criminal history records check that includes: 1. current residence, regardless of duration; 2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more; and 3. performing as much of the seven year criminal history records check as possible, if it is not possible to perform a full seven year criminal history records check.
	Verify a process to perform a seven year criminal history records check was implemented for personnel with authorized electronic access and/or authorized unescorted physical access to applicable Cyber Systems and: • A full seven year criminal history records check was completed; or • A full seven year criminal history records check was not completed, the Responsible Entity completed as much of the seven year criminal history records check as possible, and documented the reason the full seven year criminal history records check was not completed.

Auditor Notes:

R3 Part 3.3

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.

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.

Please see response to P3.1.

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-004-6, R3, Part 3.3

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that include criteria or a process to evaluate criminal history records checks for authorizing access.
	Verify the applicable criteria or process to evaluate criminal history records checks for authorizing

	access was implemented for personnel with authorized electronic access and/or authorized unescorted physical access to Applicable Systems.

Auditor Notes:

R3 Part 3.4

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

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.

Please see response to P3.1.

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-004-6, R3, Part 3.4

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that include criteria or a process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.
	Verify the criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3 was implemented.

Auditor Notes:

R3 Part 3.5

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

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.

Please see response to P3.1.

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-004-6, R3, Part 3.5

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that include a process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.
	For personnel with authorized electronic access and/or authorized unescorted physical access to Applicable Systems, verify the applicable personnel risk assessment process was implemented at least once every seven years.

Auditor Notes:

R4 Supporting Evidence and Documentation

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-6 Table R4 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations]*.

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

R4 Part 4.1

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1 Electronic access; 4.1.2 Unescorted physical access into a Physical Security Perimeter; and 4.1.3 Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

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.

Except during a CIP exceptional circumstance described in "[Program Document]", RE demonstrates authorization based on need using automated workflows in the RE application. The process for approving physical, informational or logical access entitlements are explained in "[Access Program Document]".

Authorization occurs in three separate workflows in RE, and one in Microsoft:

1. The Onboard workflow requires the individual supervisors' approval before an individual can be on boarded.

2. The Role authorization workflow is found in the document XYZ. This contains two separate approval requirements, entitlement owner(s) must approve the access and the Role Owner must approve the need.

3. The Modify/Extend Access process requires the individual supervisors' approval as well as the entitlement owners approval before an individual's access can be modified. The Supervisors' approval can be found on page X of the workflow diagram the entitlement owner's approvals can be found on page Y of the workflow diagram.

4. Authorization for access under CIP Exceptional Circumstances for MS Azure follows the Azure “Just In Time” access process shown in “[JIT Process Doc]” (also available at Link). Even in these circumstances, the RE storage area is encrypted using the RE key which would prevent access to any storage content. All items residing in the BCSI repository are encrypted with the RE key which can be rotated on demand.

To manage and authorize access to the AZURE BCSI repository RE created two parent roles “AZURE - BCSI Repository” and “Cloud Services Encryption Key Manager”. When an access role is created the workflow generates a subset of roles for user assignment; Administrator, Application User, Non Provision Admin, and Shared Accounts. This subset of roles allow users the ablity to request access to logical, physical and information access on RE resouces.

RE utilizes the workflow engine to authorize access and to provision accounts based on the subset roles an individual is assigned to.

The following files provide the RE roles that are associated with accces to the AZURE Cloud based BCSI repository.
File1 – Role for those RE personel responsible for manageing cloud Encryption Keys
File2 – Role for those RE personel authorized for administration of BCSI repository.
File3 - Role for those RE personel authorized for using the BCSI repository.
File4 - Role for those RE personel authorized for manageing the BCSI repository without the authority to provision user access.

In the MS Azure environment, access control to the BCSI content is access controlled thought encryption of the storage resource using customer-provided (RE) keys. “Screenshot” shows the configuration setting for RE-provided keys. Keys can be rotated on-demand, and on a periodic basis. Keys are stored in a key vault which no one can access except RE authorized personnel.

Additional CSP information (Azure)
Discusses how they control access to customer data.

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
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

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

Compliance Assessment Approach Specific to CIP-004-6, R4, Part 4.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access management programs which include a process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 1. Electronic access; 2. unescorted physical access into a Physical Security Perimeter; and 3. access to designated storage locations, whether physical or electronic, for BES Cyber System Information.
	If the Responsible Entity has declared and responded to CIP Exceptional Circumstances, verify the Responsible Entity has adhered to the applicable cyber security policies.
	Verify access was authorized, based on need, for: 1. Electronic access; 2. unescorted physical access into a Physical Security Perimeter; and 3. access to designated storage locations, whether physical or electronic, for BES Cyber System Information.
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.	

Auditor Notes:

R4 Part 4.2

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

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.

Quarterly verification for BCSI information stores is not required per 4.2.

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-004-6, R4, Part 4.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access management programs which include a process to verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.
	Verify the Responsible Entity has verified at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.

Auditor Notes:

R4 Part 4.3

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

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.

15 Month electronic access verification for BCSI information stores is not required per 4.3

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-004-6, R4, Part 4.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access management programs that, for electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.
	Verify the Responsible Entity has verified, at least once every 15 calendar months, that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct.
	Verify the Responsible Entity has verified, at least once every 15 calendar months, that user accounts, user account groups, or user role categories, and their specific, associated privileges are those that the Responsible Entity determines are necessary.

Auditor Notes:

R4 Part 4.4

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

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.

The RE Access Management Access Program, "[Program Document]" provides governance for the verification of information access for user accounts, user groups, or user role categories and verifies that the specific associated privileges are correct and necessary.

RE reports for the Azure roles are shown in "Report1", "Report2", "Report3", and "Report4".

The roles present in Azure (they are mapped in Section 12 of "[Program Document]") can be seen in "Screen Shot". More detail of an individual user can be seen in "Screen Shot".

Reports are generated annually to show the reviews are complete, two examples being "[EntitlementReviewReport]" and "[CloudAnnualAccessReport]". These two examples focus on Azure roles and access.

The list of designated BCSI storage locations are in "[List of storage locations]".

Additional CSP information (Azure)

By default, Azure personnel do not have access to customer storage accounts, which is controlled by Storage Account Keys generated randomly when the storage account is created or later at customer's request. Access to customer storage accounts is not needed to operate Azure. All customer data in Azure Storage or SQL Database is encrypted by default and this encryption cannot be disabled.

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-004-6, R4, Part 4.4

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access management programs that verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.
	Verify the Responsible Entity has verified, at least once every 15 calendar months, that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct.
	Verify the Responsible Entity has verified, at least once every 15 calendar months, that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are those that the Responsible Entity determines are necessary for performing assigned work functions.

Auditor Notes:

R5 Supporting Evidence and Documentation

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-6 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning]*.

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-6 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R5 Part 5.1

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

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.

RE utilizes an automated workflow to notify individuals responsible for removing physical or interactive remote access upon a termination action. The RE Access Management Program details the requirements. This applies for physical, logical, or information access. Section X shows the workflows.

Any RE employee can initiate an off boarding action using the off board option in the RE service catalog. The requester must know the employees name and if the off board is voluntary or involuntary. For involuntary requests the system will generate tasking's to disable badges (physical access), active directory accounts and removal of access for other logical and informational access during the next check run. This check runs in [workflow application] once every hour.

"Sample.pdf"is an example of an off boarding Requested Item in Access Management program for an employee with CIP physical, information and electronic access entitlements. Highlighted TASKS on the example demonstrate access removal to physical, information and electronic CIP entitlements within 24hrs. "Sample2" shows the specific task of access removal. The directory service controls access to the designated BCSI storage locations.

RE [deploys directory service] with Azure to enable users to authenticate using on-premises credentials and access resources in the cloud. If an employee is terminated, access to the Microsoft Azure Portal can be turned off simply by removing that employee from the on-premises directory service. “Screen Shot” and “Screen Shot 2” show this configuration setting in the Azure environment.

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**
[redacted]					

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

Compliance Assessment Approach Specific to CIP-004-6, R5, Part 5.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access revocation programs that include a process to initiate removal of an individual’s ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).
	Verify the Responsible Entity has: 1. initiated removal of an individual’s ability for unescorted physical access and Interactive Remote Access upon a termination action; and 2. completed the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).
Note to Auditor: Removal of the ability for access does not necessarily require removal or disabling of the individual’s accounts. The ability for access may be removed by disabling the individual’s network access, confiscation of a badge, or other suitable means. Removal of Interactive Remote Access may be accomplished, for example, by disabling the individual’s multi-factor authentication.	

Auditor Notes:

R5 Part 5.2

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

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.

RE utilizes an automated workflow for removing physical or interactive remote access upon a transfer or reassignment action. Section x of the RE Access Management Program, "[Program Doc]", details the process. The workflow is showin in Section Y.

RE supervisors, contracting officers and contracting officer representatives can request a "Modify, Extend Access Roles" action from the system catalog. The requester can remove or add access roles/entitlements, update user specific data, update an access expiration date of a contract for contract employees, and can enable or disable badge and logical access for individuals placed on extended leave, unscheduled absence, and transfer or reassignment actions.

"Adding Access", "Sample Removal", and "Sample Task" show an addition and a removal to a resource (in this case it would be Azure) as part of the process to modify user access in the event of a transfer/reassignment. Access in Azure is applied through directory service groups.

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**
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

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

Compliance Assessment Approach Specific to CIP-004-6, R5, Part 5.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access revocation programs for reassignments or transfers to revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.
	Verify the Responsible Entity has, for reassignments or transfers, revoked the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.
Note to Auditor: Revocation of access does not necessarily require removal of the individual's accounts. The account may be disabled in lieu of removal.	

Auditor Notes:

____

R5 Part 5.3

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

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.

RE utilizes an automated workflow for removing physical or interactive remote access upon a transfer or reassignment action. Section x of the RE Access Management Program, "[Program Doc]", details the process. The workflow is showin in Section Y.

RE supervisors, contracting officers and contracting officer representatives can request a "Modify, Extend Access Roles" action from the system catalog. The requester can remove or add access roles/entitlements, update user specific data, update an access expiration date of a contract for contract employees, and can enable or disable badge and logical access for individuals placed on extended leave, unscheduled absence, and transfer or reassignment actions.

"Adding Access", "Sample Removal", and "Sample Task" show an addition and a removal to a resource (in this case it would be Azure) as part of the process to modify user access in the event of a transfer/reassignment. Access in Azure is applied through directory service groups.

The list of designated BCSI storage locations are in "List of Repositories".

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-004-6, R5, Part 5.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access revocation programs for termination actions to revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5, Part 5.1), by the end of the next calendar day following the effective date of the termination action.
	Verify the Responsible Entity has, for termination actions, revoked the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.

Notes to Auditor:

1. If the access was already revoked under the actions taken for Requirement R5, Part 5.1, no further action is needed.
2. Revocation of access does not necessarily require removal or disabling of the individual's accounts. The ability for access may be removed by disabling the individual's network access, confiscation of a badge, or other suitable means.
3. Removal of Interactive Remote Access may be accomplished, for example, by disabling the individual's multi-factor authentication.

Auditor Notes:

R5 Part 5.4

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual’s non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

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.

N/A

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-004-6, R5, Part 5.4

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access revocation programs for termination

	actions to revoke the individual’s non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.
	Verify the Responsible Entity, for termination actions, has revoked the individual’s non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.
Note to Auditor: Revocation of access does not necessarily require removal of the individual’s accounts. The account may be disabled in lieu of removal.	

Auditor Notes:

____

R5 Part 5.5

CIP-0046 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: 1. Workflow or sign-off form showing password reset within 30 calendar days of the termination; 2. Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or 3. Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

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.

N/A

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-004-6, R5, Part 5.5

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access revocation programs for termination actions to change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. The documented process(es) may include provisions for the Responsible Entity to determine and document that extenuating operating circumstances require a longer time period, and may change the password(s) within 10 calendar days following the end of the operating circumstances.
	If extenuating operating circumstances are invoked, verify the circumstances are documented and include a specific end date.
	For termination actions that do not invoke extenuating operating circumstances, verify the passwords to shared accounts known to the user have been changed within 30 calendar days of the termination action.
	For termination actions that invoke extenuating operating circumstances, verify the passwords to shared accounts known to the user have been changed within 10 calendar days following the end of the extenuating operating circumstances.
	For reassignments or transfers that do not invoke extenuating operating circumstances, verify the passwords to shared accounts known to the user have been changed within 30 calendar days of the date that the Responsible Entity determines the individual no longer requires retention of the access.
	For reassignments or transfers that invoke extenuating operating circumstances, verify the passwords to shared accounts known to the user have been changed within 10 calendar days following the end of the extenuating operating circumstances.

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-004-6 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	09/17/2014	CIP RSAW Development Team	Address comments received in response to DRAFT1v0.
DRAFT3v0	12/10/2014	CIP RSAW Development Team	Address comments received in response to DRAFT2v0.
DRAFT4v0	02/06/2015	CIP RSAW Development Team	Address comments from V5R SDT and address comments in response to DRAFT3v0.
DRAFT4v1	03/06/2015	CIP RSAW Development Team	Address comments from V5R SDT meeting on March 3-4, 2015.
FINALv1	05/08/2015	CIP RSAW Development Team	Address comments from final posting; review and address comments of V5R SDT.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-011-2 – Cyber Security – Information Protection

This section to be completed by the Compliance Enforcement Authority.

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

Applicability of Requirements

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

Legend:

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

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

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

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

Findings

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

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
P1.1			
P1.2			
R2			
P2.1			
P2.2			

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 implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R1 Part 1.1

CIP-011-2 Table R1 – Information Protection			
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	Method(s) to identify information that meets the definition of BES Cyber System Information.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.

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.

- Description of responsible entity (RE) program to identify, mark, protect, and control BCSI.
- Flow chart of the information categorization process.
- List of BCSI repositories.

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**
RE provided docs here					
CSP provided documentation here if applicable.					

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

Compliance Assessment Approach Specific to CIP-011-2, R1, Part 1.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more information protection programs that have method(s) to identify information that meets the definition of BES Cyber System Information.
	Verify the Responsible Entity has implemented the method(s) to identify information that meets the definition of BES Cyber System Information.

Auditor Notes:

R1 Part 1.2

CIP-011-2 Table R1 – Cyber Security Incident Response 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	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure(s).

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.

Description of responsible entity (RE) program to identify, mark, protect, and control BCSI.
Flow chart of the information categorization process.

These sections include: sharing BCSI, awareness of surroundings, physical protection, protection over telecommunications circuits, encrypting during transit and at rest, and other requirements for best handling practices.

RE utilizes the following controls for the storage location in Azure:

- Storage location is encrypted at rest
  - Screenshot shows configuration setting
  - Logs show encryption keys can be rotated on demand by RE
- Storage location is encrypted in transmission
  - Screenshot shows encryption enabled for data in transmission
- Storage resource is access controlled
  - Screenshot shows role-based access
  - Screenshot shows directory service controls access
  - List shows user profile with more detail and tie to directory service
  - Please see CIP-004 RSAW for more detail on the RE acces control program
- Storage location only replicates to continential US
  - Screenshot shows technical policy is enabled
- Storage location is monitored for activity

  - Screenshot shows the dashboard for monitoring activity
- Storage location is monitored for policy compliance by Azure monitoring services
  - Screenshot shows a dashboard for overall compliance with policies
  - Screenshot shows the detailed policies drill-down from the top-level dashboard. These tools assist RE in detecting changes to the security configuration of its storage location

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-011-2, R1, Part 1.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more information protection programs that include procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.
	Verify the Responsible Entity has implemented the procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal. [Violation Risk Factor: Lower] [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-011-2 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R2 Part 2.1

CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	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	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.

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.

As shown in the previous response to P1.2 (narrative and evidence), the use of encryption for the storage location prevents access to the information by personnel unauthorized by RE, regardless of replication locations and deletion status of the information.

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-011-2, R2, Part 2.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media, prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the “Applicable Systems” column).
	Verify that prior to the release for reuse of Cyber Assets of Applicable Systems that contain BES Cyber System Information (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity has taken action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.

Auditor Notes:

____

R2 Part 2.2

CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	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	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.

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.

As shown in the previous response to P1.2 (narrative and evidence), the use of encryption for the storage location prevents access to the information by personnel unauthorized by RE, regardless of replication locations and deletion status of the information.

Additional CSP information (Azure)

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-011-2, R2, Part 2.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media, prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information.
	Verify that, prior to the disposal of Cyber Assets of Applicable Systems that contain BES Cyber System Information, the Responsible Entity has taken action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroyed the data storage media.

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-011-2 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	09/17/2014	CIP RSAW Development Team	Address comments received in response to DRAFT1v0.
DRAFT3v0	12/10/2014	CIP RSAW Development Team	Address comments received in response to DRAFT2v0.
DRAFT4v0	02/06/2015	CIP RSAW Development Team	Address comments from V5R SDT and address comments in response to DRAFT3v0.
DRAFT4v1	03/10/2015	CIP RSAW Development Team	Address comments from V5R SDT meeting on March 3-4, 2015.
FINALv1	05/08/2015	CIP RSAW Development Team	Address comments from final posting; review and address comments of V5R SDT.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

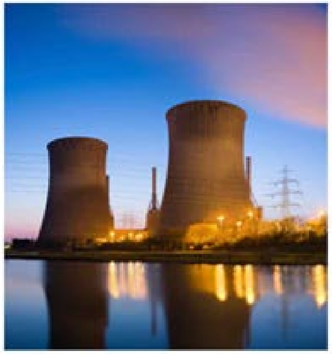
Cloud Computing Tabletop Exercise

Bulk Power System Cyber System Information

Presenters

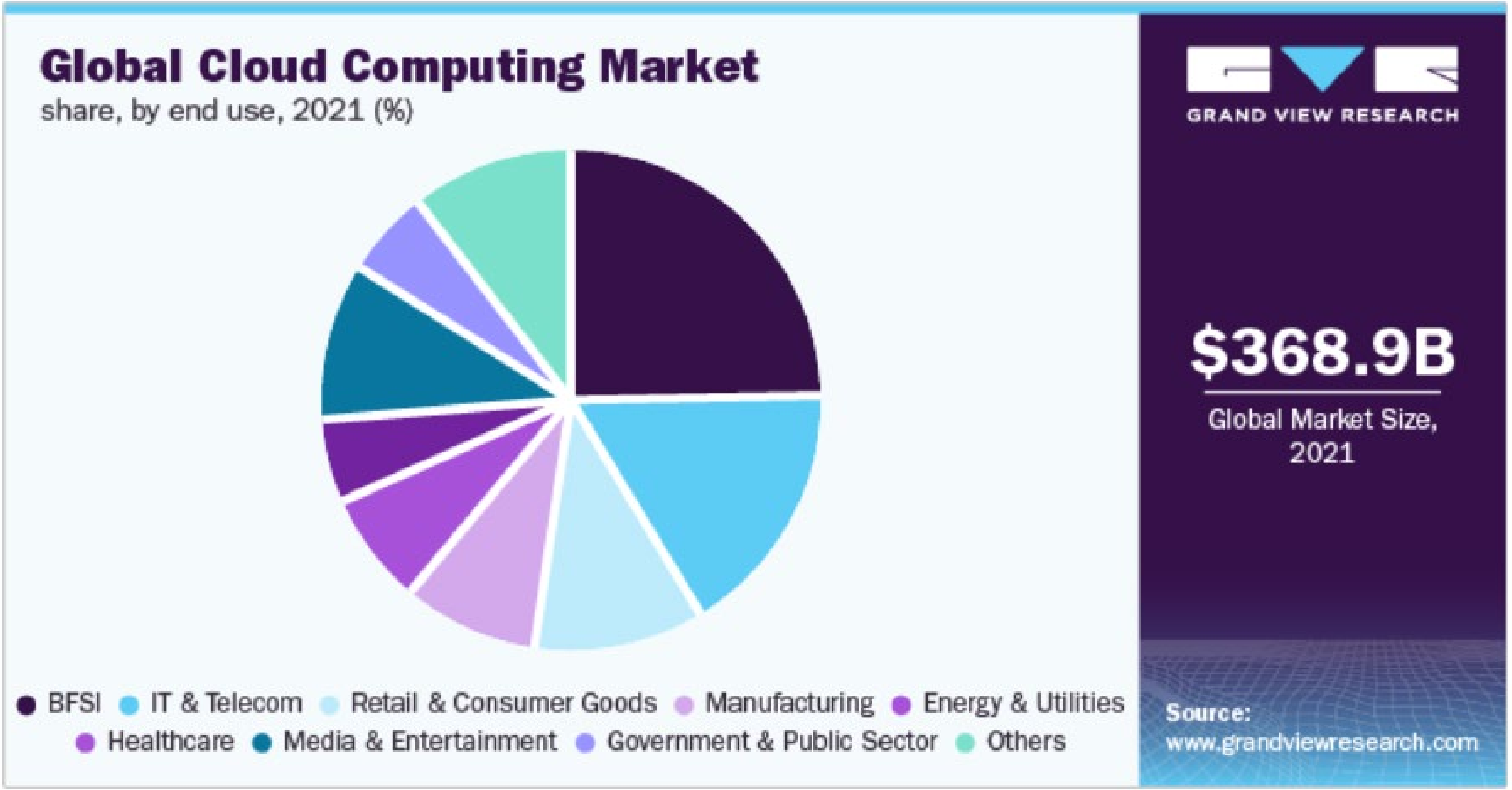
Brent Sessions (WAPA), Security Working Group Co-Chair
Morgan King (WECC), Senior Technical Advisor, Entity Monitoring
July 13, 2023

RELIABILITY | RESILIENCE | SECURITY



Cloud Adoption

[Link to recording]



Source: www.grandviewresearch.com

Participants

- Western Area Power Administration
- Microsoft
- NERC
- WECC
- MRO

Exercise Overview

- Unable to find a solid example of what a visit from an audit team may look like
- Unanswered questions about
    - Process and approach
    - What evidence looks like
    - What compliance issues might come up
    - What risk issues might come up
    - How long it takes
- Look for traps or issues that could not be resolved
- WAPA Core Value: Be Curious, Learn more, do better. Repeat.

Exercise Overview

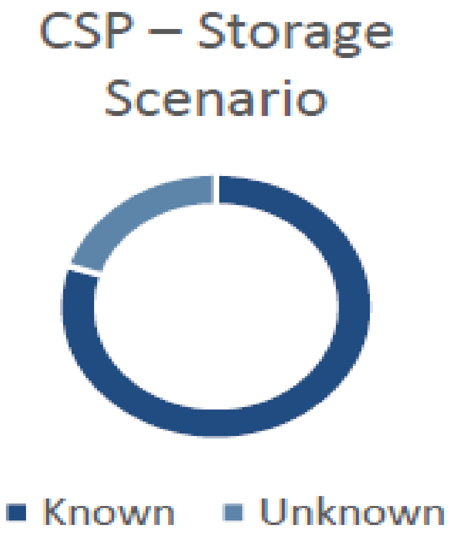
- Created a process for Responsible Entities to test their controls and determine risk issues with BCSI in the Cloud
  - Process document
  - List of what happened during the exercise
  - List of what evidence was presented and how it was relevant
  - ERO Risk Perspectives
- Shared document package that goes together to give complete picture
- 100% Virtual exercise

Exercise Scope

- Exercise conducted May 20, 2020
- Limited in scope
  - RSAW limited to CIP-004 and CIP-011
  - Reviewed to understand environment, limited depth
  - Exercise ≠ Audit or Self-Report
- **LEARNING EXPERIENCE** for ERO, WAPA, WECC, MRO and Microsoft

Exercise Overview

- Vendor-specific
- Entity-specific
- Included audit and security risk perspective
- Invaluable exchange of information between the ERO Enterprise and the [Cloud Vendor].
- Other solutions and service models should be evaluated



Example RSAWs

- Industry team led with introduction of RSAWs for CIP-004-6 and CIP-011-2
- Entity utilized vendor narrative for controls implemented in the CSP underlay environment
- RSAWs helpful in understanding the qualities/capabilities of the vendor environment
  - Two vendor documents used to guide RSAW development for this exercise:
    - NERC CIP Standards and Cloud Computing (vendor document)
    - Cloud Implementation Guide for NERC Audits (vendor document, requires vendor account)

Example RSAWs

- ERO Enterprise team notes:
  - RSAWs were underlay-focused, in addition to entity environment-specific.
  - Discussions for entity overlay around CIP-004-6 and CIP-011-2 ensued during the remainder of the exercise.

Process

1. Collaborated with WECC, MRO, NERC and Microsoft to determine best approach
2. Tabletop exercise process document, version 1.0 developed
3. Fake data and non-production environment
4. Organized and performed the exercise
5. Document the experience and use that information to improve the process – all parties
6. Create a document package with that experience for the industry
7. Rinse and repeat– take experience and feed back into the process document
8. Managed through the NERC Security Working Group and ERO

Key Takeaways

- CSP documentation found valuable to understand the cloud environment
- CSP engagement for this first exercise was essential
- Terminology differs between NERC, RE, and the CSP. Take care to make sure to describe certain functionality and environments
- RE should update their information protection program, cyber security awareness and CIP training to material to address nuances specific to cloud environments and services

Key Takeaways

- Expect a deep dive on the following items:
  - Methods used to protect BCSI in storage (at rest), in transit and use
  - Encryption key management
  - Access control, particularly as it relates to CSP personnel
  - Active Directory(ies), including updating and synchronization
  - Security control considerations not called out by the CIP standards (e.g. data sovereignty, services, etc.)
  - How unauthorized access to BCSI is prevented after cloud services are terminated.
  - Any CSP certifications that are relevant to the controls/protections being applied to secure the responsible entity's BCSI, including how those controls/protections are monitored, audited, etc.

Key Takeaways

- A schematic or compilation of the environment will be needed for the auditor to understand the environment.
- These topics need further exploration with the ERO to come to a conclusion:
  - whether "use" of data for computing is the same as "use" of BCSI (per CIP-011-2 R1.2). (Note: page 3 of the approved RSTC Security Guideline on this topic states "Data in use refers to data that is being used or modified by an end-user.")
  - whether documentation related to any relevant CSP certification and associated controls could be utilized to provide direct evidence of compliance with the applicable NERC CIP requirements.

Key Takeaways

- Product is a Technical Reference package, NOT a formal NERC Lessons Learned
- VERSION 1.0: Everyone is learning how to figure this out
- It ended up being a blend of risk and compliance questions and answers
- Everyone participated in learning, so it was a value-added exercise
- Vendor got to experience what a NERC assessment is like

Key Takeaways

- User Guide for the tabletop exercise process
  - Template format for easy preparation
  - Assessment Scope
  - Scenario Being Tested
  - Roles/Responsibilities
  - Objectives
  - Initial and follow-up activities
  - Preparation activities with timelines
  - Agenda for pre-tabletop meeting
  - Backup procedures
  - Deliverable package
  - Tips and Tricks

Key Takeaways

- The documents were endorsed by the RSTC at the March, 2023 quarterly meeting.
- The documents are a package and should be read together
- There are different owners of the document package
  - Vendor owns the CSP documentation – review any public disclosures with them
  - ERO owns their documents, so they approve separately
  - Coordination is needed between the parties, but a lot of the “dirty work” was figured out

What Else?

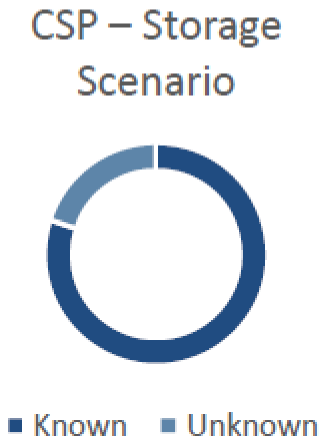
- Detailed tips for
  - Preparing for the exercise
  - RSAWs (genericized sample RSAWs are part of the package)
  - Roles and Responsibilities
  - Evidence
  - Evidence level of detail
  - CSP documentation
  - Cloud Certifications (FedRAMP)
  - Process
  - Tools and technology used
  - Chart showing relationship between Deliverable Documents
  - Table of evidence

Exercise Scope

- Limited in scope
  - Reviewed to understand environment, limited depth
  - Exercise ≠ Audit or Self-Report
- Learning experience for all participants

Exercise Overview

- Vendor-specific
- Entity-specific
- Included audit and security risk perspective
- RSAW limited to CIP-004 and CIP-011



Invaluable exchange of information between the ERO Enterprise and the [Cloud Vendor].

Other solutions and service models should be evaluated

RSAW Review

- Exercise conducted May 20, 2020
  - Industry team led with introduction of RSAWs for CIP-004-6 and CIP-011-2
  - Entity utilized vendor narrative for controls implemented in the CSP underlay environment
  - RSAWs helpful in understanding the qualities/capabilities of the vendor environment
    - Two vendor documents used to guide RSAW development for this exercise:
      - NERC CIP Standards and Cloud Computing (vendor document)
      - Cloud Implementation Guide for NERC Audits (vendor document, requires vendor account)
  - ERO Enterprise team notes:
    - RSAWs were underlay-focused, in addition to entity environment-specific.
    - Discussions for entity overlay around CIP-004-6 and CIP-011-2 ensued during the remainder of the exercise.

CIP-004-6

CIP-004-6	Audit Exercise Observations	Meets Requirement Measure
R2 Part 2.1.5 (Training on BCSI handling)	• RSAW (attestation), no vendors identified as having access to applicable to BES cyber system(s) • Vendor employees have applicable training covering all topics (in the event that access is granted to vendor employees)	✓
R4 Part 4.1.3 (Access to Designated Storage Location)	• RSAW (attestation), no vendors identified as having access • Entity has full control of access. • Issue: Vendor may have the capability to access entity data. Reference - Q&A sequence RFI-1, Q2-4, leading to RFI-2, Q1.	☒
R4 Part 4.4 (Verify access)	• RSAW (attestation), no vendors identified as having access • Evidence supports access grants are valid (multiple) • [Redact] AccessManagementProgram, p.53, and (Ref-9) vendor personnel do not have access • Issue: Active directory sync characteristics not fully described. Reference - Q&A sequence RFI-1, Q5 leading to observation	✓ With Observation
R4 Part 5.3 (Revocation)	• RSAW attestation describes methods for revocation if vendor employees had access • Entity shows full control over access with automation capability (did not exercise)	✓

CIP-011-2

CIP-011-2	Audit Exercise Observation	Meets Requirement Measure
R1 Part 1.1 (Methods to identify BCSI)	• External designated storage location (DSL) identified (Ref. 25) • Recommendation: Consider making cloud-specific procedures more explicit, ensuring that DSLs in-cloud are unambiguously identified as in-cloud	✓
R1 Part 1.2 (Procedures for BCSI)	• [Solution] activity log analytics show two users with access (procedural evidence) • Recommendation: Consider making cloud-specific procedures more explicit • Issue: Deletion of data not demonstrated. See Q&A Sequence RFI-1, Q11, following to RFI-2, Q3	☒
R2 Part 2.1	• N/A in this cloud exercise	N/A
R2 Part 2.2	• N/A in this cloud exercise	N/A

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

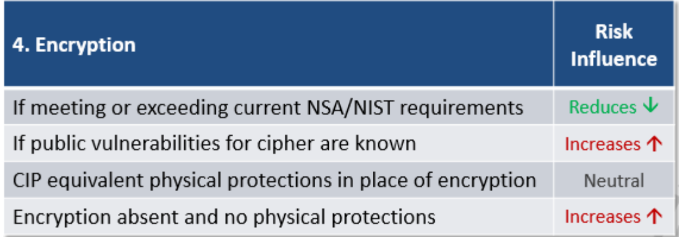
Security Risk Considerations

Risk Consideration Categories: BCSI in the Cloud

1. Business Agreements (Contracts)
2. Access/BCSI in Use
3. Service Model (Environmental Constraints)
4. Encryption
5. Certifications
6. Data sovereignty
7. Data Transformation

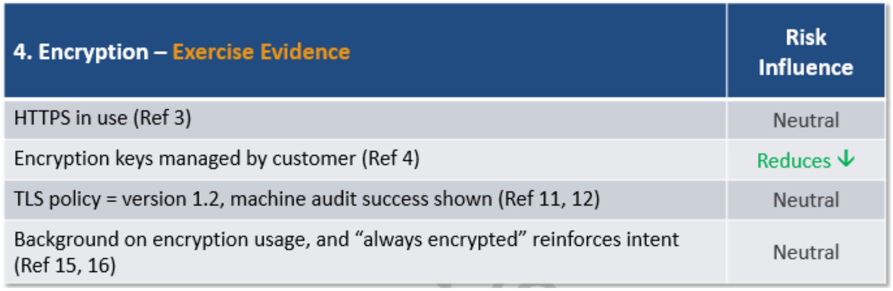
Next slides are paired:

Risk category general cloud considerations



4. Encryption	Risk Influence
If meeting or exceeding current NSA/NIST requirements	Reduces ↓
If public vulnerabilities for cipher are known	Increases ↑
CIP equivalent physical protections in place of encryption	Neutral
Encryption absent and no physical protections	Increases ↑

Cloud exercise considerations



4. Encryption – Exercise Evidence	Risk Influence
HTTPS in use (Ref 3)	Neutral
Encryption keys managed by customer (Ref 4)	Reduces ↓
TLS policy = version 1.2, machine audit success shown (Ref 11, 12)	Neutral
Background on encryption usage, and “always encrypted” reinforces intent (Ref 15, 16)	Neutral

These factors are called risk influencing factors which are understood as “a set of conditions which influence the level of specified risks related to a given activity or system”

Business Agreements

1. Business Agreements	Risk Influence	Risk if absent
Governance for vendor access to entity data	Neutral	Increases ↑
Governance for transmittal of vendor access evidence	Reduces ↓	Neutral
Declaration for encryption key management processes	Neutral	Increases ↑
Declaration for entity-specific data disposal methods	Neutral	Increases ↑
Declaration for vendor personnel background verification	Reduces ↓	Neutral
Containerization of entity content	Neutral	Increases ↑
Entity right to audit vendor or to view the details of audit results	Reduces ↓	Neutral
Notifications for access breach	Neutral	Increases ↑
General entity autonomy	Risk linked to autonomy	

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Exercise Evidence: Business Agreement

1. Business Agreements – Exercise Evidence	Risk Influence
Agreement sets obligations (Ref 1, p.3)	Neutral
Customer retains rights to data (Ref 1, p.5)	Neutral
‘Will not use’ vendor declaration (Ref 1, p.5)	Neutral
‘Will not disclose’ vendor declaration (Ref 1, p.6)	Neutral
Third-party restrictions on data access (Ref. 1, p.6)	Reduces ↓
Customer right to audit statement (Ref 1, p.8)	Neutral
Notification agreement on access breach (Ref 1, p.8)	Neutral
Notice given for changes to tertiary providers, and tertiary providers must meet or exceed the terms in the business agreement (Ref 1, p.9)	Reduces ↓
Customer will have ability to delete data (Ref 1, p.9)	Neutral
Contract agreement signed and dated (Ref 8, p.1)	Neutral

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

BCSI In Use

Three states of electronic data: At rest, in transit, and in use

What is BCSI in use?

- Consider: *Data that is processed in real-time by a Cyber Asset, and is not at rest or in transit*

2. BCSI in Use	Risk Influence
BCSI enters ‘In Use’ state within vendor infrastructure	Increases ↑
Access controls for BCSI in use	Neutral
On premise use of cloud technology	Reduces ↓
Encryption of BCSI in use (homomorphic encryption – future technology)	Reduces ↓

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Exercise Evidence: BCSI in Use

2. BCSI in Use – Exercise Evidence	Risk Influence
Confidentiality commitment (Ref 1, p.11)	Neutral
Security awareness and training for vendor employees from entity (Ref 1, p.11)	Neutral
Physical access limited to authorized personnel (Ref 1, p.11)	Neutral
Physical media containing customer data tracked (Ref 1, p.11)	Neutral
Access that is granted to vendor admins is tracked (Ref 1, p.11-12)	Neutral
Vendor access credentials automatically expire after time period (Ref 1, p.11)	Neutral
Customer controls access grant to vendor (Ref. 6) (Ref. 9)	Neutral
Trusted vendor services are permitted to access the service account. Issue: Access to backup or other service level accounts. Reference 21, p.14, Ref 21, p.16, RFI-1 Q2-Q4, and RFI-2 Q1.	Increases ↑

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Service Model

Less about:

- SaaS (Software as a Service)
- PaaS (Platform as a Service)
- IaaS (Infrastructure as a Service)

There is not much risk difference between the service models. All have the potential access to data by vendors or others.

More about:

- Limiting service provider access through infrastructure architecture
- Service composition (just storage, storage + services, tertiary providers)

3. Service Model	Risk Influence
Tertiary cloud dependencies	Increases ↑

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exercise Evidence: Service Model

3. Service Model – Exercise Evidence	Risk Influence
Vendor employees do not have access to customer data by default (Ref 1, p.9, Ref 23)	Neutral
Tertiary providers can be identified, will meet or exceed business agreement terms (Ref 1, p.9)	Reduces ↓
Customer right to terminate tertiary providers (Ref 1, p.9)	Reduces ↓
Environment is logically isolated, implemented with VLAN and firewall configurations that are controlled by the customer. (Ref 2, 10)	Neutral
Environment enforces access against a copy of the entity AD, a push architecture from entity to the cloud environment (Ref 17, 18, 19)	Neutral
AD sync timing between customer and vendor was unexplored. The sync mechanism could permit unauthorized access if synchronization controls fail or utilize periodicities longer than permitted for revocation (see Q&A Sequence, RFI-1 Q5)	(Observation)
A full configuration export of the service environment was not available for review (see Q&A Sequence, RFI-1 Q7)	(Observation)

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Encryption

Encryption is typically required in cloud environment

- Consider NSA sources and NIST requirements
- Consider cipher strength: (RSA-xxx, SHA-xxx, AES-xxx)

4. Encryption	Risk Influence
If meeting or exceeding current NSA/NIST requirements	Reduces ↓
If public vulnerabilities for cipher are known	Increases ↑
CIP equivalent physical protections in place of encryption	Neutral
Encryption absent and no physical protections	Increases ↑

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Exercise Evidence: Encryption

4. Encryption – Exercise Evidence	Risk Influence
HTTPS in use (Ref 3)	Neutral
Encryption keys managed by customer to help prevent unauthorized access (Ref 4)	Reduces ↓
TLS policy = version 1.2, machine audit success shown (Ref 11, 12)	Neutral
Background on encryption usage, and "always encrypted" reinforces intent (Ref 15, 16)	Neutral

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Certifications

- Most certifications or accreditations focus on the underlay (including access to the overlay). 3PAOs do not audit the customer data environments.
- Some certifications are objective-based. Be sure to evaluate the certification objective against CIP objectives.

5. Certifications	Risk Influence	Risk if absent
FedRAMP Certification	Neutral	Increases ↑
SOC 1 Not applicable, attestational in nature		
SOC 2 (Type 1 + Type 2) with adequacies under Security, Processing Integrity, and Confidentiality headings	Neutral	Increases ↑
SOC 3 with compliance seal	Neutral	Increases ↑
Other – draw comparisons with known certifications	Neutral	Increases ↑

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Exercise Evidence: Certifications

5. Certifications – Exercise Evidence	Risk Influence
Per business agreement, vendor follows ISO 27001, ISO 27002, ISO 27018 (Ref 1, p.7)	Neutral
Customer has access to certification reports such as FedRAMP, ISO-x, SOC, and PCI/DSS (Ref 24)	Neutral
Per business agreement, recertification performed annually by a 3PAO (Ref 1, p.8)	Reduces ↓
Latest certification reports unavailable for review due to sensitivity. In an actual audit these reports would be made available to the customer (See Q&A Sequence, RFI-1 Qx leading to RFI-2 Q4).	Increases ↑

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Data Sovereignty

Data Sovereignty: A consideration related to the potential geographic location of the data

6. Data Sovereignty	Risk Influence
Certification or business agreement declaration of US domestic only	Neutral
Certification or business agreement declaration of US or Canada domestic only (Canadian entities)	Neutral
International or undeclared	Increases ↑

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Exercise Evidence: Data Sovereignty

6. Data Sovereignty – Exercise Evidence	Risk Influence
Core services store data at rest in specified geo-locations (Ref 1, p.9)	Neutral
Location policy detail shows entity can technically enforce geo-location of the customer environment according to a list assignment (Ref 13, 14)	Neutral
Configuration parameters show US geo-locations selected for this US-based entity, and no international selections (Ref. 24)	Neutral

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Data Transformation

7. Data Transformation	Risk Influence
Encryption: A strong but reversible means to protect data	Neutral
Obfuscation: A reversible clear text replacement according to a key. Easy to reverse engineer	Increases ↑
Obfuscation in Real-time communication protocols where efficient data processing is required (typically not BCSI)	Neutral
Redaction: Some electronic redaction formats retain source content	Neutral
Sanitization: Permanent and irreversible transformation of data	Reduces ↓
Access authorizations and training on program and custody controls	Neutral

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Exercise Evidence: Data Transformation

7. Data Transformation – Exercise Evidence	Risk Influence
Vendor contractually commits to deleting entity data, backups, and cached data after customer disassociation with the vendor (Ref 20)	Neutral
Vendor provides steps for customer data deletion prior to service cancellation (Ref 22, p.1)	Neutral
Business agreement suspends customer data for a waiting period following disassociation in which the customer has no access to the data and potentially no remedy once the agreement has terminated (Ref 20)	Increases ↑
Evidence of deletion not demonstrated (See Q&A Sequence RFI-1, Q11-Q12, leading to RFI-2 Q3)	Increases ↑

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

BCSI in the Cloud
Exercise Risk Conclusions

In Summary:

Risk Considerations: BCSI in the Cloud	Risk Influence
1. Business agreements (contract agreements)	Neutral
2. Access/data in use	Increases ↑
3. Service model (environmental constraints)	Neutral (More to learn)
4. Encryption (data at rest or in transit)	Neutral
5. Certifications	Increases ↑ (Exercise Stop)
6. Data sovereignty	Neutral
7. Data transformation	Increases ↑

Background References

- ERO Enterprise CMEP Practice Guide
- 2019-02 Project Page
- CIPC Security Guideline, Cloud Computing
- Homomorphic encryption
- Data sovereignty
- Obfuscation in software
- Sanitization

Appendix A - Exercise Evidence Mapping*

1. Business Agreement
2. Isolation Choices
3. HTTPS
4. Customer Managed Keys
5. <not used>
6. Access solution
7. <not used>
8. Business Agreement Order
9. RE RFI-1
10. Network Isolation Example
11. TLS Policy 1
12. TLS Policy Shown
13. Location Policy Detail
14. Geo-Replication Policy
15. Encryption fundamentals
16. Key Vault Config
17. AD Config
18. AD Config 2
19. AD Sync
20. Subscription Cancellation
21. Trusted Services
22. Data Management
23. Data Access Management
24. RE RFI-2
25. Program Document
26. Create Resource Fail

** Note: Evidence references above are linked descriptively (mapped) to the Industry side evidence description table within "BCSI Cloud TTX Lessons Learned – Appendix B"*

Questions and Answers

NERC

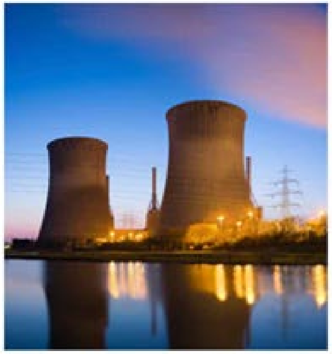
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

BCSI Cloud Storage Tabletop Exercise

ERO Enterprise Tabletop Team Members:
Lonnie Ratliff (NERC), Jess Syring (MRO), Morgan King (WECC)

August 18, 2022

RELIABILITY | RESILIENCE | SECURITY

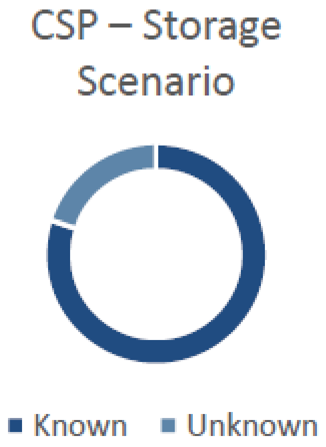


Exercise Scope

- Limited in scope
  - Reviewed to understand environment, limited depth
  - Exercise ≠ Audit or Self-Report
- Learning experience for all participants

Exercise Overview

- Vendor-specific
- Entity-specific
- Included audit and security risk perspective
- RSAW limited to CIP-004 and CIP-011



Invaluable exchange of information between the ERO Enterprise and the [Cloud Vendor].

Other solutions and service models should be evaluated

RSAW Review

- Exercise conducted May 20, 2020
  - Industry team led with introduction of RSAWs for CIP-004-6 and CIP-011-2
  - Entity utilized vendor narrative for controls implemented in the CSP underlay environment
  - RSAWs helpful in understanding the qualities/capabilities of the vendor environment
    - Two vendor documents used to guide RSAW development for this exercise:
      - NERC CIP Standards and Cloud Computing (vendor document)
      - Cloud Implementation Guide for NERC Audits (vendor document, requires vendor account)
  - ERO Enterprise team notes:
    - RSAWs were underlay-focused, in addition to entity environment-specific.
    - Discussions for entity overlay around CIP-004-6 and CIP-011-2 ensued during the remainder of the exercise.

CIP-004-6

CIP-004-6	Audit Exercise Observations	Meets Requirement Measure
R2 Part 2.1.5 (Training on BCSI handling)	• RSAW (attestation), no vendors identified as having access to applicable to BES cyber system(s) • Vendor employees have applicable training covering all topics (in the event that access is granted to vendor employees)	✓
R4 Part 4.1.3 (Access to Designated Storage Location)	• RSAW (attestation), no vendors identified as having access • Entity has full control of access. • Issue: Vendor may have the capability to access entity data. Reference - Q&A sequence RFI-1, Q2-4, leading to RFI-2, Q1.	☒
R4 Part 4.4 (Verify access)	• RSAW (attestation), no vendors identified as having access • Evidence supports access grants are valid (multiple) • [Redact] AccessManagementProgram, p.53, and (Ref-9) vendor personnel do not have access • Issue: Active directory sync characteristics not fully described. Reference - Q&A sequence RFI-1, Q5 leading to observation	✓ With Observation
R4 Part 5.3 (Revocation)	• RSAW attestation describes methods for revocation if vendor employees had access • Entity shows full control over access with automation capability (did not exercise)	✓

CIP-011-2

CIP-011-2	Audit Exercise Observation	Meets Requirement Measure
R1 Part 1.1 (Methods to identify BCSI)	• External designated storage location (DSL) identified (Ref. 25) • Recommendation: Consider making cloud-specific procedures more explicit, ensuring that DSLs in-cloud are unambiguously identified as in-cloud	✓
R1 Part 1.2 (Procedures for BCSI)	• [Solution] activity log analytics show two users with access (procedural evidence) • Recommendation: Consider making cloud-specific procedures more explicit • Issue: Deletion of data not demonstrated. See Q&A Sequence RFI-1, Q11, following to RFI-2, Q3	☒
R2 Part 2.1	• N/A in this cloud exercise	N/A
R2 Part 2.2	• N/A in this cloud exercise	N/A

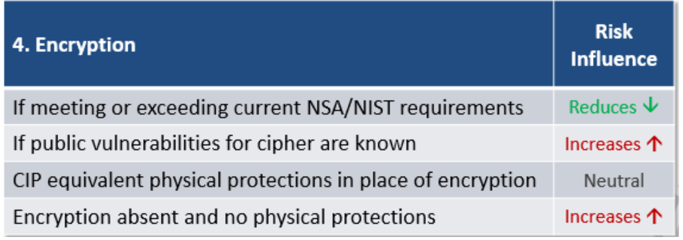
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Security Risk Considerations

Risk Consideration Categories: BCSI in the Cloud
1. Business Agreements (Contracts)
2. Access/BCSI in Use
3. Service Model (Environmental Constraints)
4. Encryption
5. Certifications
6. Data sovereignty
7. Data Transformation

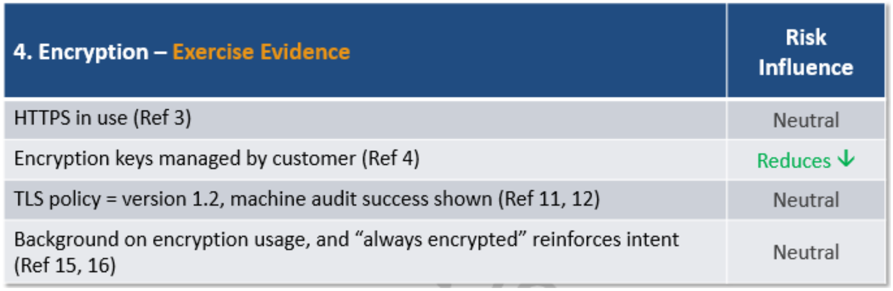
Next slides are paired:

Risk category general cloud considerations



4. Encryption	Risk Influence
If meeting or exceeding current NSA/NIST requirements	Reduces ↓
If public vulnerabilities for cipher are known	Increases ↑
CIP equivalent physical protections in place of encryption	Neutral
Encryption absent and no physical protections	Increases ↑

Cloud exercise considerations



4. Encryption – Exercise Evidence	Risk Influence
HTTPS in use (Ref 3)	Neutral
Encryption keys managed by customer (Ref 4)	Reduces ↓
TLS policy = version 1.2, machine audit success shown (Ref 11, 12)	Neutral
Background on encryption usage, and “always encrypted” reinforces intent (Ref 15, 16)	Neutral

These factors are called risk influencing factors which are understood as “a set of conditions which influence the level of specified risks related to a given activity or system”

Business Agreements

1. Business Agreements	Risk Influence	Risk if absent
Governance for vendor access to entity data	Neutral	Increases ↑
Governance for transmittal of vendor access evidence	Reduces ↓	Neutral
Declaration for encryption key management processes	Neutral	Increases ↑
Declaration for entity-specific data disposal methods	Neutral	Increases ↑
Declaration for vendor personnel background verification	Reduces ↓	Neutral
Containerization of entity content	Neutral	Increases ↑
Entity right to audit vendor or to view the details of audit results	Reduces ↓	Neutral
Notifications for access breach	Neutral	Increases ↑
General entity autonomy	Risk linked to autonomy	

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Exercise Evidence: Business Agreement

1. Business Agreements – Exercise Evidence	Risk Influence
Agreement sets obligations (Ref 1, p.3)	Neutral
Customer retains rights to data (Ref 1, p.5)	Neutral
‘Will not use’ vendor declaration (Ref 1, p.5)	Neutral
‘Will not disclose’ vendor declaration (Ref 1, p.6)	Neutral
Third-party restrictions on data access (Ref. 1, p.6)	Reduces ↓
Customer right to audit statement (Ref 1, p.8)	Neutral
Notification agreement on access breach (Ref 1, p.8)	Neutral
Notice given for changes to tertiary providers, and tertiary providers must meet or exceed the terms in the business agreement (Ref 1, p.9)	Reduces ↓
Customer will have ability to delete data (Ref 1, p.9)	Neutral
Contract agreement signed and dated (Ref 8, p.1)	Neutral

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

BCSI In Use

Three states of electronic data: At rest, in transit, and in use

What is BCSI in use?

- Consider: *Data that is processed in real-time by a Cyber Asset, and is not at rest or in transit*

2. BCSI in Use	Risk Influence
BCSI enters 'In Use' state within vendor infrastructure	Increases ↑
Access controls for BCSI in use	Neutral
On premise use of cloud technology	Reduces ↓
Encryption of BCSI in use (homomorphic encryption – future technology)	Reduces ↓

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Exercise Evidence: BCSI in Use

2. BCSI in Use – Exercise Evidence	Risk Influence
Confidentiality commitment (Ref 1, p.11)	Neutral
Security awareness and training for vendor employees from entity (Ref 1, p.11)	Neutral
Physical access limited to authorized personnel (Ref 1, p.11)	Neutral
Physical media containing customer data tracked (Ref 1, p.11)	Neutral
Access that is granted to vendor admins is tracked (Ref 1, p.11-12)	Neutral
Vendor access credentials automatically expire after time period (Ref 1, p.11)	Neutral
Customer controls access grant to vendor (Ref. 6) (Ref. 9)	Neutral
Trusted vendor services are permitted to access the service account. Issue: Access to backup or other service level accounts. Reference 21, p.14, Ref 21, p.16, RFI-1 Q2-Q4, and RFI-2 Q1.	Increases ↑

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Service Model

Less about:

- SaaS (Software as a Service)
- PaaS (Platform as a Service)
- IaaS (Infrastructure as a Service)

There is not much risk difference between the service models. All have the potential access to data by vendors or others.

More about:

- Limiting service provider access through infrastructure architecture
- Service composition (just storage, storage + services, tertiary providers)

3. Service Model	Risk Influence
Tertiary cloud dependencies	Increases ↑

Exercise Evidence: Service Model

3. Service Model – Exercise Evidence	Risk Influence
Vendor employees do not have access to customer data by default (Ref 1, p.9, Ref 23)	Neutral
Tertiary providers can be identified, will meet or exceed business agreement terms (Ref 1, p.9)	Reduces ↓
Customer right to terminate tertiary providers (Ref 1, p.9)	Reduces ↓
Environment is logically isolated, implemented with VLAN and firewall configurations that are controlled by the customer. (Ref 2, 10)	Neutral
Environment enforces access against a copy of the entity AD, a push architecture from entity to the cloud environment (Ref 17, 18, 19)	Neutral
AD sync timing between customer and vendor was unexplored. The sync mechanism could permit unauthorized access if synchronization controls fail or utilize periodicities longer than permitted for revocation (see Q&A Sequence, RFI-1 Q5)	(Observation)
A full configuration export of the service environment was not available for review (see Q&A Sequence, RFI-1 Q7)	(Observation)

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Encryption

Encryption is typically required in cloud environment

- Consider NSA sources and NIST requirements
- Consider cipher strength: (RSA-xxx, SHA-xxx, AES-xxx)

4. Encryption	Risk Influence
If meeting or exceeding current NSA/NIST requirements	Reduces ↓
If public vulnerabilities for cipher are known	Increases ↑
CIP equivalent physical protections in place of encryption	Neutral
Encryption absent and no physical protections	Increases ↑

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Exercise Evidence: Encryption

4. Encryption – Exercise Evidence	Risk Influence
HTTPS in use (Ref 3)	Neutral
Encryption keys managed by customer to help prevent unauthorized access (Ref 4)	Reduces ↓
TLS policy = version 1.2, machine audit success shown (Ref 11, 12)	Neutral
Background on encryption usage, and "always encrypted" reinforces intent (Ref 15, 16)	Neutral

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Certifications

- Most certifications or accreditations focus on the underlay (including access to the overlay). 3PAOs do not audit the customer data environments.
- Some certifications are objective-based. Be sure to evaluate the certification objective against CIP objectives.

5. Certifications	Risk Influence	Risk if absent
FedRAMP Certification	Neutral	Increases ↑
SOC 1 Not applicable, attestational in nature		
SOC 2 (Type 1 + Type 2) with adequacies under Security, Processing Integrity, and Confidentiality headings	Neutral	Increases ↑
SOC 3 with compliance seal	Neutral	Increases ↑
Other – draw comparisons with known certifications	Neutral	Increases ↑

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Exercise Evidence: Certifications

5. Certifications – Exercise Evidence	Risk Influence
Per business agreement, vendor follows ISO 27001, ISO 27002, ISO 27018 (Ref 1, p.7)	Neutral
Customer has access to certification reports such as FedRAMP, ISO-x, SOC, and PCI/DSS (Ref 24)	Neutral
Per business agreement, recertification performed annually by a 3PAO (Ref 1, p.8)	Reduces ↓
Latest certification reports unavailable for review due to sensitivity. In an actual audit these reports would be made available to the customer (See Q&A Sequence, RFI-1 Qx leading to RFI-2 Q4).	Increases ↑

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Data Sovereignty

Data Sovereignty: A consideration related to the potential geographic location of the data

6. Data Sovereignty	Risk Influence
Certification or business agreement declaration of US domestic only	Neutral
Certification or business agreement declaration of US or Canada domestic only (Canadian entities)	Neutral
International or undeclared	Increases ↑

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Exercise Evidence: Data Sovereignty

6. Data Sovereignty – Exercise Evidence	Risk Influence
Core services store data at rest in specified geo-locations (Ref 1, p.9)	Neutral
Location policy detail shows entity can technically enforce geo-location of the customer environment according to a list assignment (Ref 13, 14)	Neutral
Configuration parameters show US geo-locations selected for this US-based entity, and no international selections (Ref. 24)	Neutral

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Data Transformation

7. Data Transformation	Risk Influence
Encryption: A strong but reversible means to protect data	Neutral
Obfuscation: A reversible clear text replacement according to a key. Easy to reverse engineer	Increases ↑
Obfuscation in Real-time communication protocols where efficient data processing is required (typically not BCSI)	Neutral
Redaction: Some electronic redaction formats retain source content	Neutral
Sanitization: Permanent and irreversible transformation of data	Reduces ↓
Access authorizations and training on program and custody controls	Neutral

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Exercise Evidence: Data Transformation

7. Data Transformation – Exercise Evidence	Risk Influence
Vendor contractually commits to deleting entity data, backups, and cached data after customer disassociation with the vendor (Ref 20)	Neutral
Vendor provides steps for customer data deletion prior to service cancellation (Ref 22, p.1)	Neutral
Business agreement suspends customer data for a waiting period following disassociation in which the customer has no access to the data and potentially no remedy once the agreement has terminated (Ref 20)	Increases ↑
Evidence of deletion not demonstrated (See Q&A Sequence RFI-1, Q11-Q12, leading to RFI-2 Q3)	Increases ↑

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

BCSI in the Cloud
Exercise Risk Conclusions

In Summary:

Risk Considerations: BCSI in the Cloud	Risk Influence
1. Business agreements (contract agreements)	Neutral
2. Access/data in use	Increases ↑
3. Service model (environmental constraints)	Neutral (More to learn)
4. Encryption (data at rest or in transit)	Neutral
5. Certifications	Increases ↑ (Exercise Stop)
6. Data sovereignty	Neutral
7. Data transformation	Increases ↑

Background References

- ERO Enterprise CMEP Practice Guide
- 2019-02 Project Page
- CIPC Security Guideline, Cloud Computing
- Homomorphic encryption
- Data sovereignty
- Obfuscation in software
- Sanitization

Appendix A - Exercise Evidence Mapping*

1. Business Agreement
2. Isolation Choices
3. HTTPS
4. Customer Managed Keys
5. <not used>
6. Access solution
7. <not used>
8. Business Agreement Order
9. RE RFI-1
10. Network Isolation Example
11. TLS Policy 1
12. TLS Policy Shown
13. Location Policy Detail
14. Geo-Replication Policy
15. Encryption fundamentals
16. Key Vault Config
17. AD Config
18. AD Config 2
19. AD Sync
20. Subscription Cancellation
21. Trusted Services
22. Data Management
23. Data Access Management
24. RE RFI-2
25. Program Document
26. Create Resource Fail

** Note: Evidence references above are linked descriptively (mapped) to the Industry side evidence description table within "BCSI Cloud TTX Lessons Learned – Appendix B"*

Questions and Answers