Electric Reliability and Security for the West

Controls Guidance and Compliance Failure Points

CIP-012-1

Entity Coordination
Identity Management and Access Control

September 2022

WECC Intent

The *Controls Guidance and Compliance Failure Points* document guides registered entities in assessing risks associated with their business activities and designing appropriate internal controls in response. WECC's intent is to provide examples supporting the efforts of registered entities to design controls specific to operational risk *and* compliance with the NERC Reliability Standards. The registered entity may use this document as a starting point in assessing risk and designing appropriate internal controls. Each registered entity should perform a risk assessment to identify its entity-specific risks and design appropriate internal controls to mitigate those risks; WECC does not intend for this document to establish a standard or baseline for entity risk assessment or controls objectives.

> ***Note:*** *Guidance questions help an entity understand and document controls. Any responses, including lack of affirmative feedback, will have no consequences on an entity's demonstration of compliance during a Compliance Monitoring and Enforcement Program (CMEP) engagement.*
>
> ** Please send feedback to internalcontrols@WECC.org with suggestions on controls guidance and potential failure points questions.*

Definitions and Instructions

Control Objective: Aim or purpose of internal control to address identified risk or operational concern.

Control Activities: Policies, procedures, techniques, and mechanisms to achieve control objectives and mitigate related risks.

Quality Assurance/Quality Control (QA/QC): How an entity *verifies* it performed an activity or verifies an activity was performed *correctly* (examples include separation of duties, having a supervisor double-check someone's work, etc.).

Risk Category: Type of operational and inherent risks identified by the ERO Enterprise for use in the Compliance Oversight Plan (COP). Entities should use Risk Categories to understand, monitor, and mitigate known and future risks.

Risk Category

Entity Coordination: Coordination, internally and externally, as with third-party suppliers and contractors

before making changes to the system or taking any actions with the potential to impact another entity and, in turn, impact BPS reliability and security. Coordination should address the risk associated with operating horizon, planning horizons and during emergencies. Failure to coordinate may impact BPS reliability and security.

Identity Management and Access Control: Entities must develop controls to prevent or mitigate malicious or unintentional access to Bulk Electric System (BES) Cyber Assets. Failure to develop controls may compromise the integrity and operability of the BPS. The three major tenets of security controls are to provide confidentiality, integrity, and availability (CIA).

CIP-012-1 intends to mitigate cybersecurity risks to the reliable operation of the BES by protecting the confidentiality and integrity of Real-time Assessment (RTA) and Real-time monitoring (RTM) data transmitted between Control Centers.

Control Objective(s)

Your entity should perform a risk assessment and identify entity-specific control objectives to mitigate those risks. To help your entity get started, WECC has identified generic control objectives to mitigate the risks associated with the risk categories mentioned above and CIP-012-1. You may want to consider these three objectives:

> **Control Objective 1**: Identify applicable RTA and RTM data. (Relates to Entity Coordination)
>
> **Control Objective 2**: Define protections for RTA and RTM data transmitted between Control Centers. (Relates to Identity Management and Access Control)
>
> **Control Objective 3**: Mitigate risks posed by unauthorized disclosure and unauthorized modification of RTA and RTM data while being transmitted between Control Centers. (Relates to Identity Management and Access Control)

Reliability and Security Control Activities

Control activities are how your entity meets your control objectives. As you design controls, your entity should tailor them to entity-specific control objectives.

Below are examples of control activities based on good practices WECC has observed that are designed to meet the objectives listed above. WECC does not intend for these activities or the associated questions to be prescriptive. Rather, they should help your entity consider how you might meet your objectives in your own unique environment. They also may help your entity identify controls you did not realize you had.

Control Objective 1: Identify applicable RTA and RTM data.
Control Activity A: Identify applicable Control Centers.

1. How does your entity ensure it identifies all applicable Control Centers, including those owned by

other entities?

2. How does your entity identify any geographically separate data centers transmitting RTA and RTM data to its applicable Control Centers?
3. How does your entity identify and exempt:
    a. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission?
    b. Systems, structures, and components regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54?
    c. Control Centers that transmit to another Control Center RTA or RTM data pertaining only to the generation resource or Transmission station or substation co-located with the transmitting Control Center?
4. Does your entity include any exempted Control Centers in its mitigation measures?

Control Activity B: Identify RTA and RTM data.

1. How does your entity identify the RTA and RTM data transmitted between Control Centers?
    a. Do you base it on data requests pursuant to the data specification from TOP-003 and IRO-010 requirements?
    b. When data requests do not indicate which data is RTA and RTM data, how do you determine which data needs protection?
2. How does your entity document its identification of RTA and RTM data?
3. What QA/QC does your entity perform to ensure it correctly identifies RTA and RTM data?
4. How does your entity communicate the identified RTA and RTM data to relevant subject matter experts (SME)?

Control Activity C: Identify how RTA and RTM data is transmitted between Control Centers (communication channels).

1. How does your entity ensure it identifies all intra-entity, inter-entity, and inter-regional transmission of RTA and RTM data between applicable Control Centers?
2. How does your entity involve stakeholders in identifying how RTA and RTM data is transmitted between Control Centers?
3. How does your entity identify the infrastructure used to transmit RTA and RTM data?
    a. How do you document the infrastructure to transmit RTA and RTM data?
    b. What QA/QC do you perform to ensure you correctly identified the infrastructure to transmit RTA and RTM?
4. How does your entity identify third-party networks that transmit RTA and RTM data between Control Centers?
5. How does your entity communicate its identification of communication channels to relevant SMEs?

Control Objective 2: Define protections for RTA and RTM data transmitted between Control Centers.

Control Activity A: Identify risks posed by unauthorized disclosure and unauthorized modification of RTA and RTM data.

1. How does your entity coordinate among different departments or business units to identify the risks posed by the communication channels transmitting RTA and RTM data between Control Centers?
2. Do the risks include:
    a. Data Confidentiality?
    b. Data Integrity?
    c. Data Availability?
3. Does the analysis consider the impact and likelihood of the risk?
4. For all demarcation points where logical or physical (or both) security protections must be applied and identified, how does your entity evaluate the risks when a demarcation point is not in a Control Center owned or operated by you?

Control Activity B: Define protections for RTA and RTM data transmitted between Control Centers.

1. How does your entity design security protections to protect RTA and RTM data transmitted between Control Centers?
    a. What guidelines do you use to determine when to use logical protection and when to use physical protection?
2. How does your entity confirm protections mitigate the identified risks?
3. How does your entity incorporate into its operations control activities to protect RTA and RTM data transmitted between Control Centers?
4. How does your entity verify the effectiveness of controls designed to protect RTA and RTM data transmitted between Control Centers?
    a. Do you have someone other than the person who designed the protections verify/validate their effectiveness?
5. If different entities own or operate applicable Control Centers, how does your entity identify the responsibilities of each entity to protect RTA and RTM data transmitted between those Control Centers?
    a. How do you identify which entity is responsible for documenting and developing protections?

Control Activity C: Identify responsive steps to take if CIP Exceptional Circumstances prevent transmitting RTA and RTM data between Control Centers.

1. How does your entity address situations where CIP Exceptional Circumstances prevent it from implementing its plan to protect RTA and RTM data transmitted between any applicable Control Centers?
    a. How do you ensure relevant personnel understand protocols for CIP Exceptional

Circumstances?

2. How does your entity evaluate the implications for BPS reliability and security if it cannot transmit RTA and RTM data between Control Centers due to a failure of the transmission link?
    a. Have you developed any alternate data communications plans or protocols?

Control Objective 3: Mitigate risks posed by unauthorized disclosure and unauthorized modification of RTA and RTM data transmitted between Control Centers

Control Activity A: Assign accountability and responsibility for implementing or verifying tools to prevent unauthorized disclosure or modification of RTA and RTM data transmitted between Control Centers.

1. How does your entity determine who is accountable and responsible for implementing the plan(s) to prevent unauthorized disclosure or modification of RTA and RTM data?
2. What governance has your entity established to oversee the person(s) accountable and responsible for implementing the plan(s)?
3. How does your entity verify whether those who are accountable and responsible for monitoring the plan(s) perform activities necessary to mitigate the risk(s)?

Control Activity B: Provide sufficient funding and personnel.

1. How does your entity ensure it provides sufficient funding and personnel to mitigate risks posed by unauthorized disclosure or modification of RTA and RTM data?
2. What QA/QC processes does your entity perform to verify it provides sufficient funding and personnel to mitigate risks posed by unauthorized disclosure or modification of RTA and RTM data?

Control Activity C: Train relevant personnel regarding how to protect against unauthorized disclosure or modification of RTA and RTM data transmitted between Control Centers.

1. How does your entity identify the skill set required for personnel to protect RTA and RTM data against unauthorized disclosure or modification?
2. How does your entity identify relevant personnel to receive training on protecting RTA and RTM data transmitted between Control Centers against unauthorized disclosure or modification?
3. How does your entity develop training materials for those personnel?
4. How does your entity ensure those personnel receive appropriate training?
5. Does your entity provide initial and refresher training?
    a. If so, how frequently do you provide refresher training?
6. What QA/QC processes does your entity employ to ensure personnel receive appropriate training?

Control Activity D: Implement mitigating measures identified in the plan(s).

1. What protections (i.e., controls) does your entity use to protect RTA and RTM data transmitted between Control Centers?
2. How does your entity identify where it applied security protection to protect that data?

   a. How do you ensure you identified all devices to which controls are applied?
3. How does your entity verify the effectiveness of implemented protection methods?
   a. How frequently are security measures reviewed for effectiveness?
   b. Do you use continuous monitoring methods?
4. What QA/QC is performed to confirm security measures are implemented and effective?

Compliance Potential Failure Points

The control activities listed above are specifically targeted at mitigating risk to the reliability and security of the BPS but also promote compliance with the referenced standard. Your entity should also develop controls specifically to mitigate compliance risk. The following compliance potential failure points relate directly to compliance risk and warrant consideration.

Potential Failure Point: Failure to implement a documented plan to mitigate the risks posed by unauthorized disclosure and unauthorized modification of RTA and RTM data transmitted between applicable Control Centers.

1. Has your entity implemented a documented plan to mitigate the risk of unauthorized disclosure or modification of RTA and RTM data transmitted between applicable Control Centers?
   a. If yes, does your plan include the following:
      i. Identifying security protection to mitigate the risks posed by unauthorized disclosure and unauthorized modification of RTA and RTM data transmitted between Control Centers;
      ii. Identifying where you applied security protection for transmitting RTA and RTM data between Control Centers; and
      iii. If different entities own or operate the Control Centers, identifying the responsibilities of each entity for applying security protection to the transmission of RTS and RTM data between those Control Centers?

Potential Failure Point: Failure to have documentation demonstrating plan implementation.

1. Does your entity have documentation demonstrating it implemented its plan to mitigate the risks posed by unauthorized disclosure and unauthorized modification of RTA and RTM data transmitted between applicable Control Centers?
   a. How do you document the security protections you use for transmitting RTA and RTM data between Control Centers?
   b. Are the locations of the security protections documented?
   c. Are security measures for RTA and RTM data transmitted to Control Centers owned or operated by other Responsible Entities identified?