Communications Between Control Centers

Entity Coordination

Identity Management and Access Control

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 North American Electric Reliability Corporation (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 control 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

Control Objective: The aim or purpose of specified controls; control objectives address the risks related to achieving an entity's larger objectives.

Control Activities: The policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and address related risks.

Internal Control: The processes, practices, policies or procedures, system applications and technology tools, and skilled human capital that an entity employs to address risks associated with the reliable operation of its business. Internal control components include:

- Control Environment;
- Risk Assessment;
- Control Activities;

- Information and Communication; and
- Monitoring.

Quality Assurance / Quality Control (QA/QC): How an entity *verifies* whether 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 Electric Reliability Organization (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.

CIP-012-2 intends to mitigate cybersecurity risks to the reliable operation of the BES by protecting the confidentiality, integrity, and availability of Real-time Assessment (RTA) and Real-time monitoring (RTM) data transmitted between Control Centers.

Control Objectives

Your entity should perform a risk assessment and identify entity-specific control objectives to mitigate those risks. To help entities get started, WECC has identified generic control objectives to mitigate the risks associated with the risk categories mentioned above and CIP-012-2. You may want to consider these three objectives:

> **Control Objective 1**: Identify applicable data used in RTA and RTM. (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**: Establish protocols or procedures for use in case of a loss of timely availability of RTA or RTM data transmitted between Control Centers. (Relates to Entity Coordination, Identity

Management and Access Control)

Reliability and Security Control Activities

Control activities are how your entity meets your control objectives. When designing and developing controls, they should be tailored to meet the applicable 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 unique environment. They also may help your entity identify controls you did not realize you had.

Control Objective 1: Identify applicable data used in RTA and RTM.

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 data used in RTA and RTM 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 cybersecurity 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 exempt Control Centers in its mitigation measures?

Control Activity B: Identify data used in RTA and RTM.

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

Control Activity C: Identify how data used in RTA and RTM 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 data used in RTA and RTM?
    a. How do you document the infrastructure to transmit data used in RTA and RTM?
    b. What QA/QC do you perform to ensure you correctly identified the infrastructure to transmit data used in 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 convey 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 used to transmit 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: Design risk mitigation methods for unauthorized disclosure, unauthorized modification, and loss of communication of 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?
    b. What logical protections do you use? (e.g., data masking, encryption/decryption)

   c. What physical protections do you use?
2. How does your entity determine where to apply logical and physical protections?
   a. Are all protections within a PSP or ESP?
   b. If not, how do you ensure there are no gaps in protection?
3. How does your entity mitigate the risk of loss of the ability to communicate RTA and RTM data?
   a. Do you have alternative communication paths or systems?
   b. Do you have service agreements with carriers with high-availability provisions?
   c. Have you developed any alternate data communication plans or protocols for use during an event?
4. How does your entity confirm methods mitigate the identified risks?
   a. How frequently are security measures reviewed for effectiveness?
   b. Do you have someone other than the person who designed the protections verify/validate their effectiveness?
   c. Do you use continuous monitoring methods?
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?
   b. Do you have written agreements to ensure the security objective is met?
   c. How do you ensure there are no gaps in security or availability controls?

Control Objective 3: Establish protocols or procedures for use in case of a loss of timely availability of RTA or RTM data transmitted between Control Centers

Control Activity A: Implement processes or procedures to recover communication links.

1. What technical recovery plans are in place to recover RTA or RTM data transmission capability?
   a. Is the recovery of communications links addressed in your CIP-009 recovery plans?
2. Have you established roles and responsibilities for the restoration of RTA and RTM data transmission availability?
   a. Does this include backup personnel?
   b. Are the personnel different from those who have operating responsibilities or who have responsibilities under the Cyber Security Incident Response plan?
3. Do your recovery plans include coordination with external entities (e.g., vendors, connected entities)?
4. How does your entity train personnel in the recovery or restoration plans?

Control Activity B: Establish protocols to determine whether the outage is caused by a cybersecurity

incident.

1. How does your entity address situations that may be caused by a cybersecurity incident?
    a. How do you ensure relevant SMEs understand the protocols for responding to a cybersecurity incident?

Control Activity C: Identify responsive steps to take if CIP Exceptional Circumstances prevent the timely transmission of 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?

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, unauthorized modification, and loss of availability, of data used in RTA and RTM while such data is being transmitted between any applicable Control Centers.

1. Does your plan include all five subparts of Requirement 1?

Potential Failure Point: Failure to correctly identify the applicable data and associated communications channels.

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 measures you use for transmitting data used in RTA and RTM 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?