WECC

Electric Reliability and Security for the West

Internal Controls

Failure Points and Guidance Questions

CIP-009-6

Security Objective

- Develop, document, and distribute a recovery plan to organization-defined personnel or roles that addresses—
  - Purpose,
  - Scope,
  - Roles,
  - Responsibilities,
  - Management commitment,
  - Coordination among organizational entities, and
  - Compliance.
  - Develop procedures to set in place a recovery response policy and its associated recovery response controls, reviews, and updates.
- Coordinate recovery response testing with organizational elements responsible for related plans.
  - Back up system-level information in the information system as frequently as defined by the organization, consistent with recovery time and recovery point objectives, and protect the confidentiality, integrity, and availability of backup information at storage locations.

NIST Special Publication 800-53 (Rev. 4) CP-9

WECC Intent

The potential failure points and guidance questions give direction to registered entities for assessment of risk, while designing internal controls specific to NERC Reliability Standards and Requirements. The Registered Entity may use this document as a starting point in determining entity risk. It is not WECC's intent to establish a standard or baseline for entity risk assessment or controls design.

Note: *Guidance questions help an entity understand and document its controls. Any responses, including lack of affirmative feedback, will have no consequences on an entity's demonstration of compliance at audit.*

**Please send feedback to* ICE@WECC.org *with suggestions on potential failure points and guidance questions.*

Potential Failure Points and Guidance Questions

CIP-009-6 R1

Potential Failure Point: Failure to develop a procedure that guides the development of recovery plans.

1. What is your process to ensure that recovery plans are comprehensive and effective?
2. How do you ensure the plan elements are comprehensive and properly maintained to include language that identifies conditions for activating recovery plans?
3. Have you engaged a team of internal and external SMEs have knowledge in the requisite disciplines, but also in the specific, contextual language and intention of CIP-009-6?
    a. For example, consider NERC guidance references *(NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011).*

Potential Failure Point: Failure to define criteria used to develop conditions for activation.

1. How do you document the conditions or circumstances under which the plan should be activated and the team mobilized?
    a. Does that documentation include information about unacceptable disruption levels?
2. Does the plan assume that not all incidents happen suddenly; some escalate at a slower pace before they are recognized as an incident? (For example, threats of industrial action, medical issues, and supply chain disruption or shortages due to environmental or economic impacts.)

Potential Failure Point: Failure to define roles and responsibilities of recovery process operation.

1. How do you document roles and responsibilities?
    a. Do the roles include all potential and appropriate stakeholders?
        i. Do privileged users understand their roles and responsibilities?
        ii. Do third-party stakeholders understand their roles and responsibilities?
        iii. Do senior executives understand their roles and responsibilities?
        iv. Do physical and information security personnel understand their roles and responsibilities?
    b. Does your plan include alternates for each role and responsibility?
2. How do you communicate roles and responsibilities?
    a. How do you ensure alternates are trained, aware, and that they understand recovery processes?
3. Have you assessed the skills of the individuals assigned to roles and does the assessment include enough alternates (internal and external)?
    a. Have the frequency and effectiveness of training and awareness sessions been considered and do those sessions increase the level of awareness and understanding of recovery processes?
4. How are the members of the response team authorized and capable to respond to an incident at the appropriate level(s)?

Potential Failure Point: Failure to define backup and storage methods of information required for system recovery.

1. How do you ensure all methods of backup and storage are included in plans?
   a. How do you document backup and storage methods?
   b. Do you use the information collected during risk assessments or business impact analysis processes to identify the available backup and storage strategies for your operations capabilities and technology?
2. Do you identify supply chain issues for suppliers and customers that may affect the requirement or definition of backup and storage methods and recovery strategy?

Potential Failure Point: Failure to define acceptance criterion for backup verifications.

1. How do you know whether backups are complete?

Potential Failure Point: Failure to develop methods to detect backup failures.

1. When a backup fails, how do you inform stakeholders of failures?
   a. How do stakeholders identify backup failures and false positives?
      i. How does the stakeholder ensure backup failures are tracked and resolved?

Potential Failure Point: Failure to outline specific response procedures for backup failures.

1. How do SMEs know how to respond to backup failures?
2. How do you document responses?
3. How do you review and update response procedures?
4. How do stakeholders ensure backup storage practices and activities for resolution of failures effectively determine whether potential incidents were identified, reviewed, and resolved?

Potential Failure Point: Failure to develop methods to preserve data.

1. How do you document preservations?
2. How are SMEs trained on methods to preserve data?
   a. Data-at-rest is protected
   b. Data-in-transit is protected
3. How do you manage assets during removal, transfers, and disposition?
4. Do you prioritize data resources (e.g., hardware, devices, data, and software) based on their classification, criticality, and business risk or value?
5. Do you share the effectiveness of methods to preserve data with appropriate stakeholders?

Potential Failure Point: Failure to develop methods suitable for cause determination.

1. Have you defined a criterion to use when determining cause?
   a. Is it based on an industry standard?

2. How do you ensure cause determinations are addressed with systematic remedies to avoid future issues?

Potential Failure Point: Failure to develop criteria to determine data preservation

1. How have you defined these terms?
   a. Are terms based on an industry standard?
2. How do you ensure identified impedance or restrictions determinations are addressed with systematic remedies to avoid future issues?

CIP-009-6 R2

Potential Failure Point (R2, R3): Failure to clearly define or communicate start and end dates used to establish timeframes for testing and updates.

1. How do you track testing?
2. How do you ensure the timeframes for testing and updates are monitored and shared with appropriate stakeholders?

Potential Failure Point: Failure to define and communicate testing methods or strategy to responsible parties required to perform testing.

1. How do your business units coordinate testing efforts?
2. How is a decision made to select one of the options for testing?
3. How do you ensure all plans are tested?
4. How do you ensure the relevant legal and regulatory requirements have been identified and considered adequately in your strategy?

Potential Failure Point: Failure to define a representative sample of information used to recover.

1. Have you defined a process or criterion for identifying a representative sample used for testing?
2. How do you ensure you have identified and considered all relevant legal and regulatory requirements in your sampling strategy?

Potential Failure Point: Failure to develop a tracking method of actual recovery instances.

1. How would you know if an actual recovery has occurred?
2. How does verification of information used in recovery occur?

Potential Failure Point: Failure to develop a criterion used to define usability of information used to recover.

1. How do you verify compatibility with current configurations?

Potential Failure Point: Failure to develop a criterion used to define an operational exercise.

1. How have you defined an operational exercise?

Potential Failure Point: Failure to develop a criterion used to define an environment representative of the production environment.

1. How have you defined an environment representative of the production environment?
2. Do you have development and testing environments that are separate from the production environment?

CIP-009-6 R3

Potential Failure Point: Failure to develop tracking process for changes of plan requiring action.

1. How have you documented and educated employees on procedures that outline tracking progress, including:
   a. All users;
   b. Privileged users;
   c. Third-party stakeholders;
   d. Senior executives; and
   e. Physical and information security personnel?
2. How have your personnel and partners provided cybersecurity awareness education and adequate training to perform their duties related to information security consistent with policies, procedures, and agreements?
3. How have you ensured you have considered the relevant legal and regulatory requirements in the policy?
4. How have you confirmed that personnel are familiar with their roles, responsibilities, and authority in response to an incident?
5. How do you validate the technical, logistical, and administrative aspects of the plans?

Potential Failure Point: Failure to define a notification criterion for plan updates.

1. How do you document notifications?
2. Do you distribute updated documentation using formal version control processes?
3. Do you manage maintenance promptly, requiring regular reports that identify progress of planned maintenance, highlight areas of weakness, and make recommendations for improving the process?