Security Objective

Awareness of access events that report on:

- Successful login attempts;
- A limit of [organization-defined number] consecutive invalid login attempts by a user during a [organization-defined period];
- A maximum number of unsuccessful login attempts; and
- Awareness of detection of malicious code.

NIST Special Publication 800-53 (Rev. 4) SI-3(1) & AU-12

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 serve to help an entity understand and document its controls. Any responses, including lack of affirmative feedback, will have no consequences to 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 & Guidance Questions

Potential Failure Point: (R4) Failure to develop a complete list of assets that require a process to log relevant events.

1. How does [the entity] ensure all applicable assets are addressed in a process to log relevant events?

Potential Failure Point: (R4) Failure to develop a procedure or process that defines events at the device or system level for the specified types.

1. How has [the entity] defined failed access attempts?
2. How has [the entity] defined failed login attempts?
3. Has [the entity] defined what constitutes malicious code?

4. How are line-of-business personnel trained on these procedures and processes?

Potential Failure Point: (R4) Failure to develop a procedure or process that outlines how the entity will capture events.

1. Does [the entity] have a procedure on how each device or system type should be configured to log events?
2. Where logging is accomplished through manual review, has [the entity] developed methods (such as specifying a scope) to minimize report size?
3. Does [the entity] have a procedure or process to ensure that devices between the Cyber Asset and log server are allowing the logging traffic to pass through?
4. Does [the entity] have a process or procedure to ensure log storage does not fill to 100 percent, which will prevent any more logs to be captured?
5. How does [the entity] ensure logging configurations (device and system) stay in place?
6. How are line-of-business personnel trained on these procedures and processes?

Potential Failure Point: (R4) Failure to develop a procedure or process that defines an "alert."

1. Has [the entity] defined who should receive alerts?
    a. What was [the entity's] process to define which security events require an alert?
    b. What mechanism(s) is used to notify responsible personnel of an alert?
        i. When an alert generated, how has [the entity] documented what actions should be taken to respond to the alert?
    c. How would [the entity] determine whether alerts have been missed or whether action was delayed?
2. How has [the entity] ensured alert configurations (device and system) stay in place?
3. How are line-of-business personnel trained on these procedures and processes?

Potential Failure Point: (R4) Failure to develop a procedure or process that defines a "failure of event logging."

1. Does [the entity] define logging failure at the device and system levels?

Potential Failure Point (R4) Failure to develop a policy that requires event log retention at the device or system level for the specified types.

1. How has [the entity] enforced this policy?
2. How has [the entity] ensured log data is properly retained?
    a. What mechanism(s) determine the log data is free from tampering or compromise?
    b. What retrieval method is used to effectively use historical data?
3. How has [the entity] ensured log retention configurations (device and system) stay in place?
4. How are line-of-business personnel trained on these procedures and processes?

Potential Failure Point (R4) Failure to develop a procedure or process that defines "technical feasibility."

1. How are technical feasibility determinations documented?

Potential Failure Point (R4) Failure to define a qualifying "CIP Exceptional Circumstance."

1. How has [the entity] defined criteria to determine whether a CIP Exceptional Circumstance exists?

Potential Failure Point (R4) Failure to define a "summarization" or a "sample."

1. How has the [the entity] defined a summarization?
2. How has the [the entity] defined a sample?

Potential Failure Point (R4) Failure to define an "undetected Cyber Security Incident."

1. How has the [the entity] defined an undetected Cyber Security Incident?

Potential Failure Point (R4) Failure to develop a procedure or process that outlines how the identification of an undetected Cyber Security Incident is to occur.

1. How has [the entity] provided guidance on methods or processes to detect incidents?
2. How are line-of-business personnel trained on these procedures and processes?

Potential Failure Point (R4) Failure to clearly define or communicate start and end dates used to establish a period for review of log outside of alert monitoring.

1. How has the [the entity] ensured log data is reviewed in a timely manner?
2. How are verifications of vulnerability mitigations documented?