



MICAD LIMITED
Advanced Industrial Security Supervisor Training

Lesson 3.4: Activity - Compliance Audit Plan: Access Control Policy - SunPeak Solar Power Substation

1. Introduction:

This document outlines a plan for conducting a compliance audit of the access control policy at the hypothetical SunPeak solar power substation. The audit aims to verify adherence to the policy, identify any gaps or weaknesses, and recommend improvements to enhance the overall security posture.

2. Policy Under Audit:

Access Control Policy (Version 1.1, dated October 26, 2024)

3. Audit Objectives:

- Verify that physical and logical access controls are implemented and functioning correctly.

- Assess the effectiveness of access control procedures in preventing unauthorized access.
- Identify any gaps or weaknesses in the access control system.
- Assess compliance with relevant regulations and industry best practices.
- Recommend improvements to enhance the effectiveness of the access control system.

4. Audit Scope:

This audit will cover the following areas:

Physical Access Control: Perimeter security (fencing, gates, lighting), building access (doors, keycard readers, biometric scanners), restricted areas (control room, server room, transformer yard).

Logical Access Control: User account management (creation, modification, deletion), access control lists (ACLs), multi-factor authentication (MFA) implementation, network security devices (firewalls, intrusion detection systems).

Documentation: Review of access control policies, procedures, and related documentation.

Personnel: Interviews with selected personnel to assess their understanding and compliance with access control procedures.

5. Audit Methodology:

The audit will employ a combination of methods:

Document Review: Examination of access control policies, procedures, and related documentation to verify compliance with established guidelines.

System Testing: Verification of the functionality of physical and logical access control systems, including testing of keycard readers, biometric scanners, and network security devices.

Observation: On-site observation of access control procedures to assess their implementation in practice.

Interviews: Interviews with selected personnel (security staff, IT staff, operations personnel) to assess their understanding and compliance with access control procedures.

Log Review: Examination of access logs to identify any suspicious activity or non-compliance.

6. Audit Timeline:

Task	Start Date	End Date	Duration	Assigned To
Planning & Preparation	November 4, 2024	November 7, 2024	4 days	John Smith
Document Review	November 8, 2024	November 11, 2024	4 days	Jane Doe
System Testing	November 12, 2024	November 15, 2024	4 days	Robert Jones
Observation	November 16, 2024	November 18, 2024	3 days	Security Team
Interviews	November 19, 2024	November 22, 2024	4 days	John Smith
Log Review	November 23, 2024	November 25, 2024	3 days	Jane Doe
Report Writing & Review	November 26, 2024	November 29, 2024	4 days	John Smith & Jane Doe

7. Reporting Procedures:

A comprehensive audit report will be prepared, including:

- Executive Summary: A concise overview of the audit's findings.
- Methodology: A description of the audit methods used.

- Findings: A detailed description of any compliance issues or gaps identified.
- Recommendations: Specific recommendations for improvement.
- Appendix: Supporting documentation (e.g., interview transcripts, test results).

The report will be submitted to senior management for review and action.

8. Resources:

- Audit team (John Smith - Security Supervisor, Jane Doe - IT Security Specialist, Robert Jones - Operations Manager, and the Security Team)
- Necessary tools and software for system testing and log review.

This plan provides a framework for a comprehensive access control compliance audit. The timeline and resources can be adjusted based on the specific context of the SunPeak substation. Remember that regular audits are crucial for maintaining a strong security posture. This detailed plan is suitable for submission to the discussion panel, allowing for discussion of different audit approaches and best practices.

