AuditScripts

Auditing Physical Security

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Physical Security

AuditScripts 5 Crucial Questions (v2.2)

Purpose:

Organizations audit their information security stance to protect the confidentiality, integrity, and availability of their information systems. Auditing and assessment allow an organization to validate their compliance with the standards they have set for themselves and to measure the levels of risk they are currently accepting.

AuditScripts has created the "5 Crucial Questions" series of audit checklists to provide auditors with a list of the five most important questions to ask when auditing a specific scope. Heavily influenced by the 20 Critical Security Controls project, these questions should serve as the starting point for any assessment.

5 Crucial Questions to Ask:

When performing an audit of an organization's physical security controls, auditors should consider at a minimum asking the following questions:

1. Are appropriate physical access controls in place at each of the organization's locations?
2. Are appropriate physical camera monitoring systems in place at each of the organization's locations?
3. Are appropriate physical security personnel in place at each of the organization's locations?
4. Do users at each of the organization's locations utilize proper identification systems at all times?
5. Have each of the organization's physical locations been properly architected to resist physical theft or destruction?

Standards References

CIS Critical Controls (v6.1):
1

NERC CIP (v5):
CIP-006-5

NIST 800 Series:
Not Applicable

NIST 800-53 (rev4):
PE-1—19

COBIT 5:
APO13, DSS05

ISO 27000:2013:
A.11

NIST Cybersecurity Framework:
ID.AM-1, PR.AC-2, PR.IP-5, DE.CM-2

IIA GTAGs:
Not Applicable

PCI DSS (v3.1):
9

HIPAA / HITECH:
HIPAA 164.310(d)(1)

Other Standards:
All current FIPS Publications (especially FIPS 140-2)