AuditScripts

Auditing Remote Access

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Remote Access

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 remote access systems, auditors should consider at a minimum asking the following questions:

1. Are only authorized individuals able to access remotely the organization's information systems?
2. Is two-factor authentication required for all individuals remotely accessing the organization's information systems?
3. Are users only able to access data assets and systems remotely that are approved for remote access?
4. Do devices used to connect to the organization remotely follow the same security standards as internal systems?
5. Is logging for remote access performed and are the logs regularly reviewed for irregular activities?

Standards References

CIS Critical Controls (v6.1):
3, 4, 5, 12

NERC CIP (v5):
CIP-005-5

NIST 800 Series:
NIST SP 800-46
NIST SP 800-47
NIST SP 800-77
NIST SP 800-114
NIST SP 800-120

NIST 800-53 (rev4):
AC-17

COBIT 5:
APO13, DSS05

ISO 27000:2013:
AC-17

NIST Cybersecurity Framework:
PR.AC-3, PR.MA-2

IIA GTAGs:
Not Applicable

PCI DSS (v3.1):
1, 2, 4, 10

HIPAA / HITECH:
Not Applicable

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