AuditScripts

Auditing Account and Identity Management

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Account and Identity Management

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 account and identity management systems, auditors should consider at a minimum asking the following questions:

1. Does a baseline of users who need access to an information system exist for each system?
2. Is each user account configured to access only the systems necessary to perform their job requirements?
3. Has each user account been properly authorized according to the organization's authorization standards?
4. Do business owners validate the user accounts under their responsibility on a regular basis?
5. Does an automated process exist for comparing the baseline of user accounts to the accounts configured on each system?

Standards References

CIS Critical Controls (v6.1):
1, 5, 11, 13, 14, 16

NERC CIP (v5):
CIP-004-5

NIST 800 Series:
Not Applicable

NIST 800-53 (rev4):
AC-1—24, PE-2—8

COBIT 5:
APO13, DSS05

ISO 27000:2013:
11.1—3

NIST Cybersecurity Framework:
PR.AC-1, DE.CM-7

IIA GTAGs:
GTAG 9

PCI DSS (v3.1):
7, 8

HIPAA / HITECH:
HIPAA 164.308(a)(1)
HIPAA 164.312(a)(4)
HIPAA 164.312(c)(1)
HIPAA 164.312(d)

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