AuditScripts

Auditing Access Control and Authorization

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Access Control and Authorization

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 ability to ensure that only proper individuals have access to sensitive resources, auditors should consider at a minimum asking the following questions:

1. Does an access control baseline exist for all data sets that details the appropriate permissions for each user who needs access to the resource?
2. Does an access control baseline exist that documents the permissions necessary for each data set?
3. Have users only been assigned the appropriate permissions to the data sets necessary to complete their job requirements?
4. Do proper authorizations exist for each user granted rights to each of the organization's data sets?
5. Does an automated validation process exist to ensure that only proper users have the proper rights to each data set?

Standards References

CIS Critical Controls (v6.1):
1, 3, 4, 5, 10, 12, 13, 14, 16, 20

NERC CIP (v5):
CIP-004-5

NIST 800 Series:
AC-1-24, PE 2-8

NIST 800-53 (rev4):
IA-7, MP-4, MP-5, SC-8, SC-9, SC-1, SC-12, SC-13, SC-28

COBIT 5:
APO13, DSS05

ISO 27000:2013:
10.8, 10.9, 12.3

NIST Cybersecurity Framework:
ID.AM-1, PR.AC-1, PR.AC-2, PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-1, PR.DS-2, PR.PT-3, PR.PT-4

IIA GTAGs:
GTAG 9

PCI DSS (v3.1):
1, 7

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

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