AuditScripts

Auditing Network Security and Monitoring

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Network Security and Monitoring

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 network security and monitoring, auditors should consider at a minimum asking the following questions:

1. Has the organization defined an information flow that baselines what network services are allowed to travel to which parts of the network?
2. Has the organization been segmented using access control lists to limit network access to only appropriate zones?
3. Is encryption used to protect sensitive data passing over all network segments (including internal)?
4. Are network monitoring tools in use to monitor for inappropriate/malicious traffic?
5. Are data loss prevention tools in place to monitor for inappropriate data sets entering or leaving the network?

Standards References

CIS Critical Controls (v6.1):
1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 15, 16, 18

NERC CIP (v5):
CIP-005-5

NIST 800 Series:
NIST SP 800-41
NIST SP 800-54
NIST SP 800-94
NIST SP 800-13

NIST 800-53 (rev4):
AC-4, PE-19, SC-1—34, SI-4

COBIT 5:
APO13, DSS05

ISO 27000:2013:
A.13, A.15, A.12, A.14

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

IIA GTAGs:
Not Applicable

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

HIPAA / HITECH:
HIPAA 164.312(e)(1)

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