Auditing An Audit Program

AuditScripts 5 Crucial Questions (v2.2)

Auditing An Audit Program

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 audit program, auditors should consider at a minimum asking the following questions:

1. Do auditors utilize a risk-based approach to auditing information systems?
2. Do auditors examine the organization in light of compliance and regulatory requirements?
3. Do auditors examine the organization in light of documented, business-defined security controls?
4. Do auditors directly report risk findings to senior executives?
5. Are auditors independent and free from undue influence when reporting risk to senior executives?

Standards References

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

NERC CIP (v5):
Not Applicable

NIST 800 Series:
NIST SP 800-53A
NIST SP 800-70
NIST SP 800-84
NIST SP 800-115
NIST 800-137

NIST 800-53 (rev4):
CA-1—7

COBIT 5:
MEA01, MEA02, MEA03

ISO 27000:2013:
Not Applicable

NIST Cybersecurity Framework:
Not Applicable

IIA GTAGs:
GTAG 3-5 & 11

PCI DSS (v3.1):
11

HIPAA / HITECH:
HIPAA 164.308(a)(8)

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