AuditScripts

Auditing Penetration Testing

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Penetration Testing

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 penetration testing processes, auditors should consider at a minimum asking the following questions:

1. Has the organization documented a detailed standard for penetration testing (including the how and when aspects)?
2. Are only appropriate users authorized to perform penetration tests on the organization's systems?
3. Are penetration tests being performed on a regular basis from both inside and outside of the organization's network?
4. Has a metric or scoring system been implemented for penetration testing to help prioritize remediation efforts?
5. Are the results of penetration tests integrated into the organization's overall risk management program?

Standards References

CIS Critical Controls (v6.1):
12, 15, 18, 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 SP 800-137

NIST 800-53 (rev4):
CA-1—7

COBIT 5:
MEA01, MEA02, MEA03

ISO 27000:2013:
12.6

NIST Cybersecurity Framework:
ID.RA-1

PCI DSS (v3.1):
11

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

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