AuditScripts

Auditing Vulnerability Management

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Vulnerability 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 vulnerability management systems, auditors should consider at a minimum asking the following questions:

1. Has the organization deployed a Security Content Automation Protocol (SCAP) scanner to identify all system weaknesses?
2. Is the organization's SCAP scanner configured to perform authenticated scans for configuration and coding weaknesses?
3. Are automated vulnerability scans performed at least weekly against each of the organization's systems?
4. Has remediation of all known weaknesses been performed in a timely manner on each of the organization's systems?
5. Is long-term trending of vulnerabilities recorded and reported regularly to all appropriate business owners?

Standards References

CIS Critical Controls (v6.1):
1, 4, 11, 15, 18, 20

NERC CIP (v5):
CIP-010-1

NIST 800 Series:
NIST SP 800-51
NIST SP 800-117
NIST SP 800-126

NIST 800-53 (rev4):
CA-1—7, RA-5, SI-2

COBIT 5:
MEA01, MEA02, MEA03

ISO 27000:2013:
Not Applicable

NIST Cybersecurity Framework:
ID.RA-1, ID.RA-2, ID.RA-5, PR.IP-12, DE.CM-8, RS.MI-3

IIA GTAGs:
GTAG-6

PCI DSS (v3.1):
11

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

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