AuditScripts

Auditing Certification and Accreditation

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Certification and Accreditation

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 certification and accreditation processes, auditors should consider at a minimum asking the following questions:

1. Is there a defined process for certifying and accrediting the organization's information systems?
2. Are both technical and governance controls included in the documented certification and accreditation process?
3. Are business owners defined for all business systems utilizing the certification and accreditation process?
4. Have system-specific baselines been created for each system prior to being placed into the production environment?
5. Have all systems been certified and accredited prior to being placed into the production environment?

Standards References

CIS Critical Controls (v6.1):
1, 2, 3, 7, 11, 12, 15, 18

NERC CIP (v5):
CIP-002-5

NIST 800 Series:
NIST SP 800-117

NIST 800-53:
Not Applicable

COBIT 5:
APO13, DSS04

ISO 27000:2013:
Not Applicable

NIST Cybersecurity Framework:
ID.AM-1, ID.AM-2, ID.AM-3, ID.BE-4, PR.IP-1, PR.IP-2, PR.IP-3

IIA GTAGs:
Not Applicable

PCI DSS (v3.1):
6

HIPAA / HITECH:
Not Applicable

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