AuditScripts

Auditing Governance

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Governance

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 security governance processes, auditors should consider at a minimum asking the following questions:

1. Have senior executives documented and approved a charter for the organization's information security program?
2. Has the organization created an information systems steering committee to manage the governance process?
3. Have appropriate policies and procedures been documented to define security controls for the organization?
4. Has the organization's staff been properly trained in the organization's standards for information security?
5. Are appropriate budgets for information security regularly approved for the organization?

Standards References

CIS Critical Controls (v6.1):
3

NERC CIP (v5):
CIP-003-5

NIST 800 Series:
Not Applicable

NIST 800-53 (rev4):
CM-1—9, PL-1—6, SA-1—14, SI-1, SI-5, SI--6, PM-1—11

COBIT 5:
EDM01—05, APO01—13, BAI01—10, DSS01, DSS03, DSS06

ISO 27000:2013:
A.5, A.6, A.7, A.18

NIST Cybersecurity Framework:
ID.BE-3, ID.GV-1, ID.GV-2, ID.GV-3, ID.GV-4, PR.AT-4, PR.IP-5, PR.IP-6, PR.IP-7, PR.IP-8, PR.IP-9, PR.IP-10 PR.IP-11, PR.IP-12, PR.PT-1 PR.PT-2, DE.DP-2, DE.DP-5

IIA GTAGs:
GTAG-1
GTAG-15
GTAG-17

PCI DSS (v3.1):
12

HIPAA / HITECH:
HIPAA 164.308(a)(1)
HIPAA 164.308(a)(2)
HIPAA 164.308(b)(1)

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