AuditScripts

Auditing Risk Management

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Risk 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 risk management practices, auditors should consider at a minimum asking the following questions:

1. Has the organization adopted a risk assessment and management methodology for their information systems?
2. Have all appropriate personnel been trained and are involved in the risk management process?
3. Have data owners been assigned to all information assets, and have they assigned criticality levels to all assets?
4. Has a complete risk assessment been performed recently (within the past twelve months)?
5. Have risk remediation steps been identified and acted upon as a result of the organization's recent risk assessments?

Standards References

CIS Critical Controls (v6.1):
4

NERC CIP (v5):
CIP-005-5

NIST 800 Series:
NIST SP 800-46
NIST SP 800-47
NIST SP 800-77
NIST SP 800-114
NIS TSP 800-120

NIST 800-53 (rev4):
RA-1—5, PM-9

COBIT 5:
EDM03, APO012

ISO 27000:2013:
A.11

NIST Cybersecurity Framework:
ID.AM-5, ID.BE-2, ID.BE-3
ID.BE-4, ID.BE-5, ID.GV-4
ID.RA-1, ID.RA-2, ID.RA-3
ID.RA-4, ID.RA-5, ID.RA-6
ID.RM-1, ID.RM-2, ID.RM-3,
PR.IP-7, PR.IP-8, DE.AE-4

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

PCI DSS (v3.1):
12

HIPAA / HITECH:
Not Applicable

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