AuditScripts

Auditing Training, Education, and Awareness

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Training, Education, and Awareness

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 education program, auditors should consider at a minimum asking the following questions:

1. Has the organization defined a documented standard for training and educating all personnel on information security related job roles and responsibilities?
2. Has a specific education plan been created for all types of workforce members?
3. Is each employee's education recorded and regularly compared to the requirements for their job role?
4. Are all users trained on a baseline set of security skills?
5. Are scenario based/social engineering exercises performed regularly to evaluate the effective of education programs?

Standards References

CIS Critical Controls (v6.1):
17, 18, 19

NERC CIP (v5):
CIP-004-05

NIST 800 Series:
NIST SP 800-16
NIST SP 800-50

NIST 800-53 (rev4):
AT-1—5

COBIT 5:
APO07

ISO 27000:2013:
Not Applicable

NIST Cybersecurity Framework:
PR.AT-1, PR.AT-2, PR.AT-3
PR.AT-4, PR.AT-5, RS.CO-1

IIA GTAGs:
Not Applicable

PCI DSS (v3.1):
12

HIPAA / HITECH:
HIPAA 164.308(a)(5)

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