AuditScripts

Auditing Social Media

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Social Media

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 use of social media platforms, auditors should consider at a minimum asking the following questions:

1. Has the organization documented a standard for how personnel can or should use social media platforms?
2. Is access to only authorized social media platforms allowed via web content filtering technologies?
3. Does the organization's anti-malware software detect web-based threats that originate via social media?
4. Are the organization's personnel trained on the appropriate use of social media and the dangers of improper use?
5. Are social engineering exercises regularly performed via social media to test personnel on the appropriate use of the platforms?

Standards References

CIS Critical Controls (v6.1):
Not Applicable

NERC CIP (v5):
Not Applicable

NIST 800 Series:
Not Applicable

NIST 800-53 (rev4):
Not Applicable

COBIT 5:
APO13, DSS05

ISO 27000:2013:
Not Applicable

NIST Cybersecurity Framework:
Not Applicable

IIA GTAGs:
Not Applicable

PCI DSS (v3.1):
Not Applicable

HIPAA / HITECH:
Not Applicable

Other Standards:
Not Applicable