AuditScripts

Auditing Internet Security and Use

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Internet Security and Use

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 internet use practices, auditors should consider at a minimum asking the following questions:

1. Are only authorized users in the organization allowed to connect to the internet?
2. Are authorized users only able to access specific network protocols (web, ssl, etc.) on the internet?
3. Are content filters in place to limit internet access to only required business content?
4. Are authenticated proxy servers in place to proxy all internet traffic to only authorized internet users?
5. Is malicious internet traffic blocked at the organization's network boundary?

Standards References

CIS Critical Controls (v6.1):
2, 8

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