AuditScripts

Auditing System Decommissioning

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing System Decommissioning

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 standard for decommissioning systems, auditors should consider at a minimum asking the following questions:

1. Does a documented standard exist for the process of decommissioning the organization's systems?
2. When repurposing or destroying systems, is the organization's system decommissioning standard followed?
3. Prior to system decommissioning, is an appropriate backup of all the system's data performed and archived?
4. Are all hard disks and data storage devices effectively wiped of all data prior to device destruction?
5. Is a log maintained of all devices and when data wiping or destruction occurs for each device?

Standards References

CIS Critical Controls (v6.1):
Not Applicable

NERC CIP (v5):
CIP-011-1

NIST 800 Series:
NIST SP 800-88

NIST 800-53 (rev4):
Not Applicable

COBIT 5:
APO13, DSS05

ISO 27000:2013:
Not Applicable

NIST Cybersecurity Framework:
PR.DS-3, PR.IP-6

IIA GTAGs:
Not Applicable

PCI DSS (v3.1):
3

HIPAA / HITECH:
HIPAA 164.310(c)(1)
HIPAA 164.312(d)(1)

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