AuditScripts

Auditing Encryption

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Encryption

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 encryption and it's ability to insure the integrity and confidentiality of the data, auditors should consider at a minimum asking the following questions:

1. Are older, less secure encryption algorithms such as the Data Encryption Standard (DES) or MD5 in use in the organization?
2. Are symmetric encryption algorithms with keys less than 112 bit in use in the organization?
3. Is a standard for key management documented and strictly followed in the organization for all encryption keys?
4. Is all highly sensitive data stored by the organization properly encrypted?
5. Is all highly sensitive data transmitted by the organization properly encrypted?

Standards References

CIS Critical Controls (v6.1):
10, 11, 13, 14, 15

NERC CIP (v5):
Not Applicable

NIST 800 Series:
NIST SP 800-21, 22
NIST SP 800-25, 29
NIST SP 800-32, 57, 111
NIST SP 800-130 – 133

NIST 800-53 (rev4):
IA-7, MP-4, MP-5, SC-8, SC-9, SC-11, SC-12, SC-13, SC-28

COBIT 5:
APO13, DSS05

ISO 27000:2013:
10.8, 10.9, 12.3

NIST Cybersecurity Framework:
Not Applicable

IIA GTAGs:
Not Applicable

PCI DSS (v3.1):
2, 3, 4, 6, 7

HIPAA / HITECH:
HIPAA 164.310(d)(1)
HIPAA 164.312(a)(1)
HIPAA 164.312(e)(1)
HITECH 170.202
HITECH 170.205
HITECH 170.210

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