AuditScripts

Auditing Control Exception Standards

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Control Exception Standards

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 security control exception process, auditors should consider at a minimum asking the following questions:

1. Does a documented process exist for circumstances where exceptions must be made to security controls?
2. Do business owners have to personally apply for and take responsibility for requested exceptions?
3. Does a senior executive (such as the CIO) also have to approve all exceptions to security controls?
4. Are all exception requests approved only for a limited period and renewed only after a regular review process?
5. Does a central database of all approved exceptions exist that auditors and business owners can query?

Standards References

CIS Critical Controls (v6.1):
5, 7, 11

NERC CIP (v5):
R3

NIST 800 Series:
Not Applicable

NIST 800-53 (rev4):
Not Applicable

COBIT 5:
Not Applicable

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