AuditScripts

Auditing Configuration Management and Change Management

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Configuration Management and Change Management

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 configuration management and change management processes, auditors should consider at a minimum asking the following questions:

1. Does the organization have a documented effective configuration management and change management process defined?
2. Is the organization following the configuration management and change management process it defined for itself?
3. Does a change management board exist, made up of staff from diverse parts of the organization?
4. Is a documented emergency change management process defined for the organization?
5. Has the process for configuration management and change management been effectively communicated to the organization?

Standards References

CIS Critical Controls (v6.1):
2, 3, 5, 7, 11, 13, 15

NERC CIP (v5):
Not Applicable

NIST 800 Series:
Not Applicable

NIST 800-53 (rev4):
CM-1—9

COBIT 5:
BAI06. BAI07, BAI10

ISO 27000:2013:
Not Applicable

NIST Cybersecurity Framework:
PR.IP-1, PR.IP-2, PR.IP-3, DE.AE-1

IIA GTAGs:
GTAG-2

PCI DSS (v3.1):
Not Applicable

HIPAA / HITECH:
Not Applicable

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