AuditScripts

Auditing Incident Management

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Incident 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 incident management program, auditors should consider at a minimum asking the following questions:

1. Does the organization have a detailed, documented incident response plan in place?
2. Has the organization's incident response plan been approved and endorsed by senior management?
3. Are the roles of all classes of organizational staff defined in the incident response plan?
4. Have contact plans been established for engaging law enforcement during an incident?
5. Have incident handlers and staff been properly trained in technical capabilities for handling incidents?

Standards References

CIS Critical Controls (v6.1):
19

NERC CIP (v5):
CIP-008-5

NIST 800 Series:
NIST SP 800-61
NIST SP 800-86

NIST 800-53 (rev4):
IR-1—8

COBIT 5:
DSS02

ISO 27000:2013:
A.16

NIST Cybersecurity Framework:
PR.IP-9, PR.IP-10, DE.AE-4
DE.AE-5, DE.DP-4, RS.RP-1
RS.CO-1, RS.CO-2, RS.CO-3
RS.CO-4, RS.CO-5, RS.AN-1
RS.AN-2, RS.AN-3, RS.AN-4
RS.MI-1, RS.MI-2, RS.MI-3
RS.IM-1, RS.IM-2, RC.RP-1
RC.IM-1, RC.IM-2, RC.CO-1
RC.CO-2, RC.CO-3

IIA GTAGs:
Not Applicable

PCI DSS (v3.1):
Not Applicable

HIPAA / HITECH:
HIPAA 164.308(a)(6)

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