Auditing Email Security

AuditScripts 5 Crucial Questions (v2.2)

These materials are considered sensitive and confidential materials and may not be used for any purpose other than the organization’s own internal use. This material may not otherwise be shared, used, reproduced, or disseminated outside of the organization in any way without prior written permission.

Auditing Email Security

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 email systems, auditors should consider at a minimum asking the following questions:

1. Are all email systems configured according to the organization’s standards for that email software?
2. Are all email systems up-to-date with the latest version of the email software?
3. Are anti-spam and anti-malware systems used only to allow appropriate emails to reach the organization’s systems?
4. Are only appropriate users granted access to the organization’s email systems?
5. Does the email system perform content filtering to allow only appropriate content in or out of the organization?

Standards References

CIS Critical Controls (v6.1):
2, 7, 8

NERC CIP (v5):
CIP-007-5 R2, CIP-010-5 R2

NIST 800 Series:
SP 800-45
SP 800-49

NIST 800-53 (rev4):
SI-8

COBIT 5:
APO13, DSS05

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)