AuditScripts

Auditing Data Classification

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Data Classification

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 data classification processes, auditors should consider at a minimum asking the following questions:

1. Has the organization defined data classification levels for the organization?
2. Are guidelines provided to data owners for how to classify resources and examples of datasets at each level?
3. Are business owners involved in defining the classification levels of their data systems?
4. Are data classification levels kept current and reviewed for each dataset on a regular basis?
5. Are the organization's security controls based on the classification level of the information system?

Standards References

CIS Critical Controls (v6.1):
3, 13, 14, 16

NERC CIP (v5):
CIP-002-5

NIST 800 Series:
NIST SP 800-60

NIST 800-53 (rev4):
AC-4

COBIT 5:
APO13, DSS05

ISO 27000:2013:
A.9

NIST Cybersecurity Framework:
ID.AM-1, ID.AM-3, ID.AM-5, ID.BE-2, ID.BE-4, ID.BE-5, PR.DS-1, PR.DS-2

IIA GTAGs:
Not Applicable

PCI DSS (v3.1):
3, 7

HIPAA / HITECH:
Not Applicable

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