AuditScripts

Auditing Database Security

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Database 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 database systems, auditors should consider at a minimum asking the following questions:

1. Have all database systems been configured according to the organization’s standard for that database software?
2. Is all database software up-to-date with the latest version of database software?
3. Have database-specific vulnerability scanners regularly been used against the database?
4. Are only appropriate users granted access to database objects on the server?
5. Is database object ownership (admin rights) limited to only those users who absolutely need that right?

Standards References

CIS Critical Controls (v6.1):
1, 2, 3, 5, 14, 16, 18

NERC CIP (v5):
Not Applicable

NIST 800 Series:
Not Applicable

NIST 800-53 (rev4):
Not Applicable

COBIT 5:
APO13, DSS05

ISO 27000:2013
Not Applicable

NIST Cybersecurity Framework:
PR.DS-4, PR.DS-7

IIA GTAGs:
Not Applicable

PCI DSS (v3.1):
Not Applicable

HIPAA / HITECH:
Not Applicable

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