



Auditing Data Backup and Archiving

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 Data Backup and Archiving

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

1. Has an information inventory been created defining all data sets that need to be backed up?
2. Are backups for all data sets being performed on a regular basis as defined by the data owner?
3. Are all backups being tested for integrity on a regular basis?
4. Are all data backups encrypted in transit and while at rest?
5. Are all data backups stored in a physically secure environment?

©AuditScripts.com & Enclave Security, LLC under a Creative Commons Attribution-NonCommercial 3.0 Unported (CC BY-NC 3.0) License.

http://creativecommons.org/licenses/by-nc/3.0/deed.en_US.

Standards References

CIS Critical Controls (v6.1):
2, 3, 10, 14

NERC CIP (v5):
Not Applicable

NIST 800 Series:
NIST SP 800-21, 22
NIST SP 800-25, 29
NIST SP 800-32, 57, 111
NIST SP 800-130 – 133

NIST 800-53 (rev4):
IA-7, MP-4, MP-5, SC-8, SC-9,
SC-11, SC-12, SC-13, SC-28

COBIT 5:
APO13, DSS05

ISO 27000:2013:
10.8, 10.9, 12.3

NIST Cybersecurity Framework:
ID.BE-5, PR.IP-4

IIA GTAGs:
Not Applicable

PCI DSS (v3.1):
2, 3, 4, 6, 7

HIPAA / HITECH:
HIPAA 164.310(d)(1)
HIPAA 164.312(a)(1)
HIPAA 164.312(e)(1)
HITECH 170.202
HITECH 170.205
HITECH 170.210

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

