AuditScripts

Auditing Business Continuity and Disaster Recovery (BCP/DR)

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Business Continuity and Disaster Recovery (BCP/DR)

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 BCP/DR plans, auditors should consider at a minimum asking the following questions:

1. Has the organization performed a comprehensive asset inventory and assigned business owners to all assets?
2. Has the organization performed a Business Impact Analysis (BIA) as a part of their BCP/DR plans?
3. Have all the organization's personnel been trained in their role in the BCP/DR process?
4. Are all BCP/DR plans tested and kept up-to-date on a regular basis?
5. Is the organization regularly backing up their information systems onsite and offsite in light of their BCP/DR plans?

Standards References

CIS Critical Controls (v6.1):
10

NERC CIP (v5):
CIP-009-5

NIST 800 Series:
NIST SP 800-34

NIST 800-53 (rev4):
CP-1—10

COBIT 5:
DSS04

ISO 27000:2013:
A.17

NIST Cybersecurity Framework:
ID.BE-5, ID.RA-4, DE.AE-4, 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:
GTAG 10

PCI DSS (v3.1):
Not Applicable

HIPAA / HITECH:
HIPAA 164.308(a)(7)

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