AuditScripts

# Auditing Third Party and Cloud Security

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

# Auditing Third Party and Cloud 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 allows 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 security standards for third parties, auditors should consider at a minimum asking the following questions:

1. Has the organization documented an approval process for sharing data with third party business partners?
2. Do contracts document the security requirements for business partners to follow when protecting the organization's data?
3. Do contracts define Service Level Agreements (SLAs) for business partners to follow to meet the goals of the contract?
4. Do all business partner contracts include a right-to-audit clause to ensure proper protection of the organization's data?
5. Is the organization's data encrypted when passing over untrusted or third party networks?

## Standards References

**CIS Critical Controls (v6.1):**
Not Applicable

**NERC CIP (v5):**
Not Applicable

**NIST 800 Series:**
NIST SP 800-144
NIST SP 800-145
NIST SP 800-146

**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:**
6.2, 10.2

**NIST Cybersecurity Framework:**
ID.AM-1, ID.AM-4, ID.AM-6, ID.BE-1, PR.AT-3, DE.CM-6

**IIA GTAGs:**
GTAG-7

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

**HIPAA / HITECH:**
HIPAA: 164.308(b)(1)

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