AuditScripts

# Auditing Personnel Security

AuditScripts 5 Crucial Questions (v2.2)



SECURITY enclave

# Auditing Personnel 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 personnel security controls, auditors should consider at a minimum asking the following questions:

1. Are only authorized personnel documented and granted access to the organization's data assets?
2. Are background checks performed against all of the organization's personnel prior to granting access?
3. Are personnel properly trained in their responsibilities and in protecting the organization's data prior to being granted access to the organization's data?
4. Are personnel termination practices documented and strictly and quickly performed upon personnel termination?
5. Is access to the organization's data assets regularly reviewed to ensure that only authorized individuals have access?



### Standards References

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

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

**NIST 800 Series:**
Not Applicable

**NIST 800-53 (rev4):**
PS-1—8

**COBIT 5:**
APO07, APO08, APO13

**ISO 27000:2013:**
8.1, 8.2, 8.3

**NIST Cybersecurity Framework:**
PR.IP-11, DE.CM-3, DE.DP-1, RS.CO-1,

**IIA GTAGs:**
Not Applicable

**PCI DSS (v3.1):**
12

**HIPAA / HITECH:**
HIPAA 164.308 (a)(3)

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