AuditScripts

# Auditing Workstation Security

AuditScripts 5 Crucial Questions (v2.2)



SECURITY enclave

# Auditing Workstation 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 workstations, auditors should consider at a minimum asking the following questions:

1. Has a documented standard been created for the security configuration of each type of workstation in the organization?
2. Does each device utilize whitelisting software to ensure that only appropriate software executes on the system?
3. Does each device utilize anti-malware software to limit the execution of malicious code on the system?
4. Does each device utilize a host-based firewall to limit potential network attacks directed against the system?
5. Are only authorized users local administrators of each of the organization's workstations?



### Standards References

**CIS Critical Controls (v6.1):**
1, 2, 3, 5, 8, 13, 16

**NERC CIP (v5):**
CIP-007-5

**NIST 800 Series:**
NIST SP 800-68
NIST SP 800-69
NIST SP 800-83
NIST SP 800-111
NIST SP 800-147
NIST SP 800-167

**NIST 800-53 (rev4):**
AC-7—16, MA-1—6

**COBIT 5:**
APO13, DSS05

**ISO 27000:2013:**
11.5, 12.4

**NIST Cybersecurity Framework:**
ID.AM-1, ID.AM-2

**IIA GTAGs:**
Not Applicable

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

**HIPAA / HITECH:**
164.310(b)
164.310(c)
164.310(d)(1)

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