AuditScripts

# Auditing Mobile Devices

## AuditScripts 5 Crucial Questions (v2.2)



SECURITY enclave

# Auditing Mobile Devices

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 mobile devices, auditors should consider at a minimum asking the following questions:

1. Are only authorized mobile devices in use by the organization able to store or process sensitive data?
2. Are all mobile devices utilizing whole disk encryption to protect the data on the systems?
3. Is strong authentication required in order to logon to all mobile devices – including phones and tablets?
4. Do all mobile devices follow approved security configuration standards that are approved by the organization?
5. Are all employees properly trained to handle mobile devices to limit loss through physical theft?



## Standards References

**CIS Critical Controls (v6.1):**
1, 2, 3, 12, 13, 14, 15

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

**NIST 800 Series:**
NIST SP 800-19
NIST SP 800-72
NIST SP 800-83
NIST SP 800-101
NIST SP 800-111
NIST SP 800-124
NIST SP 800-163
NISTSP 800-164

**NIST 800-53 (rev4):**
AC-19

**COBIT 5:**
APO13, DSS05

**ISO 27000:2013:**
A.8, A.15

**NIST Cybersecurity Framework:**
ID.AM-1, ID.AM-2, PR.AC-3

**IIA GTAGs:**
Not Applicable

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

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

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