



# Auditing Removable Media

AuditScripts 5 Crucial Questions (v2.2)

These materials are considered sensitive and confidential materials and may not be used for any purpose other than the organization's own internal use. This material may not otherwise be shared, used, reproduced, or disseminated outside of the organization in any way without prior written permission.



# Auditing Removable Media

## 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 removable media security, auditors should consider at a minimum asking the following questions:

1. Is only authorized removable media able to be used successfully on the organization’s systems?
2. Is auto-run disabled for all removable media to limit the spread & execution of malicious code?
3. Is authorized removable media encrypted in order to protect the data in storage on the device?
4. Is host-based data loss prevention in use to limit what content can be transferred to authorized removable media devices?
5. Are logs recorded and alerts generated on the use of removable media (authorized or unauthorized)?

©AuditScripts.com & Enclave Security, LLC under a Creative Commons Attribution-NonCommercial 3.0 Unported (CC BY-NC 3.0) License.

[http://creativecommons.org/licenses/by-nc/3.0/deed.en\\_US](http://creativecommons.org/licenses/by-nc/3.0/deed.en_US).

## Standards References

**CIS Critical Controls (v6.1):**  
8, 13

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

**NIST 800 Series:**  
NIST SP 800-111

**NIST 800-53 (rev4):**  
MP-1–6

**COBIT 5:**  
APO13, DSS05

**ISO 27000:2013:**  
A:8

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

**IIA GTAGs:**  
Not Applicable

**PCI DSS (v3.1):**  
3

**HIPAA / HITECH:**  
HIPAA 164.310(d)(1)  
HITECH 170.210

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

