



# Auditing Software Updates

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 Software Updates

## 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 software update practices, auditors should consider at a minimum asking the following questions:

1. Is an inventory of all authorized software used by the organization created and up to date?
2. Are application whitelisting tools in use to ensure that only authorized software versions are in use?
3. Are automatic software update tools in place for automatically installing updates for all software on a regular basis?
4. Is testing performed on all software updates prior to deployment in a production environment?
5. Are vulnerability scanning tools used to validate the proper installation of software updates on all systems?

©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):

1, 2, 3, 4, 7, 11, 12, 18

### NERC CIP (v5):

CIP-007-5

### NIST 800 Series:

NIST SP 800-40

### NIST 800-53 (rev4):

SI-3, SI-5, SI-7

### COBIT 5:

APO13, DSS05

### ISO 27000:2013:

Not Applicable

### NIST Cybersecurity Framework:

ID.AM-2

### IIA GTAGs:

GTAG-2

### PCI DSS (v3.1):

5, 6

### HIPAA / HITECH:

HIPAA 164.310(c)(1)

### Other Standards:

All current FIPS Publications (especially FIPS 140-2)

