AuditScripts

Auditing Software Development

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Software Development

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 development practices, auditors should consider at a minimum asking the following questions:

1. Has the organization adopted a formal Software Development Lifecycle (SDLC) to use when developing new applications?
2. Has the organization standardized on a code development platform to use when developing applications?
3. Are developers trained in secure coding practices for the coding language adopted by the organization?
4. Are code scanning tools in use in the organization to scan source code for potential weaknesses?
5. Are development and production environments separated and controls in place to ensure that only properly tested and approved code is allowed onto production systems?

Standards References

CIS Critical Controls (v6.1):
2, 3, 4, 5, 7, 9, 18

NERC CIP (v5):
Not Applicable

NIST 800 Series:
NIST SP 800-95

NIST 800-53 (rev4):
SA-1—14, SI-7, SI-9—13

COBIT 5:
BAI02

ISO 27000:2013:
A.15

NIST Cybersecurity Framework:
ID.AM-2, PR.DS-7

IIA GTAGs:
GTAG-8
GTAG-14

PCI DSS (v3.1):
2, 3, 4, 6

HIPAA / HITECH:
Not Applicable

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