# AuditScripts

# Auditing Business Applications Security

AuditScripts 5 Crucial Questions (v2.2)

# enclave
SECURITY

# Auditing Business Applications 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 business application systems, auditors should consider at a minimum asking the following questions:

1. Are clear business requirements defined each time custom business applications are developed or implemented?
2. Is appropriate security always defined as a business requirement for business application systems?
3. Does the organization utilize a documented software development lifecycle when developing all applications?
4. Does the organization utilize code review tools when developing custom code for the enterprise?
5. Are Web Application Firewalls (WAFs) used to protect all web-based applications?

## Standards References

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

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

**NIST 800 Series:**
NIST SP 800-64
NIST SP 800-70

**NIST 800-53 (rev4):**
SA-1−14, SI-7−13

**COBIT 5:**
APO13, BAI02, DSS05

**ISO 27000:2013:**
12.2, 12.5

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

**IIA GTAGs:**
GTAG 8 & 14

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

**HIPAA / HITECH:**
Not Applicable

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