CPA CHARTERED PROFESSIONAL ACCOUNTANTS

WebTrust Certifying Authorities AUDIT

Presented by

DIGITAL AGE STRATEGIES PVT. LTD.

Business With Wisdom
...Growth With Assurance

What is Web Trust Audit

Audit Definition:

Audit conducted by an independent WebTrust-accredited auditor, to ensure compliance with all the WebTrust security, accounting, audit trail, confidentiality, business, and legal requirements.

The WebTrust audit covers the validation processes that are followed to obtain identity as well as a large amount of technical security configuration and management.

WebTrust review includes both privacy and security but also includes confidentiality, transaction integrity, business practice disclosures.

Audit Types: As per ISAE 3000 (International Standard on Assurance Engagements) WebTrust for CA Audit

Assurance engagements include both **Attestation engagements (Attestation Audit)**, in which a party (Third Party Independent Auditor) other than the practitioner measures or evaluates the underlying subject matter against the criteria, and **Direct engagements (Opinion Audit)**, in which the practitioner (Auditor) measures or evaluates the underlying subject matter against the criteria.

What does Web Trust Audit Covers

Audit Coverage:

- The WebTrust Program for Certification Authorities helps to ensure that a CA is properly following its Certification Practice Statement, properly verifying organizations, and properly protecting its certificate keys.
- The audit specifically verifies that a particular certificate authority Discloses its key and certificate life cycle management business and information privacy practices and provides such services in accordance with its disclosed practices.
- CAs maintain effective controls to provide reasonable assurance:
  - Subscriber information is properly authenticated
  - The integrity of keys and certificates it manages are established and protected throughout their life cycles
  - Subscriber and relying party information is restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
  - The continuity of key and certificate life cycle management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity based on the AICPA/CICA WebTrust for Certification Authorities criteria

Why WebTrust for CAs

WebTrust For CAs ensure that:

- Proper procedures are followed in activities involving e-commerce transactions, public key infrastructure (PKI), and cryptography.
- In Online Trust and e-commerce transactions, Confidentiality, Authenticity, Integrity and Nonrepudiation are followed complying to PKI and SSL Certificate security requirements.
- Customer concerns about privacy, security, business practices addressed and signifies that CA meets independent standards for the issuing and managing digital certificates.

SCOPE OF WORK & OUT OF SCOPE

Broad Scope:

- Digital Signature certificate
- e-Sign

Out of Scope:

- SSL Certification,
- Code Signing,
- Extended Validation,
- OV (Organization Validation) Certificate,
- DV (Domain Validation) Certificates,
- VMC (Verified Marc Certificates)

AUDIT APPROACH

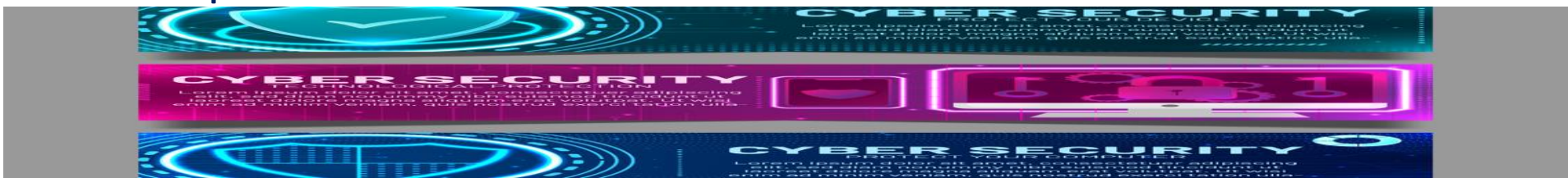
Audit Steps:

WebTrust Audit not Prescriptive (CPA Canada does not insist or provide any Checklist or Questionnaire for Audit)

A. Understand the scope, look for security Control requirements references suggested by CPA Canada / WebTrust and Baseline requirement document of CA Browser forum, prepare customized checklist. (300+ Page Checklist for DSC & e-Sign) See Sample.

B. Conduct WebTrust Audit with detailed/Comprehensive checklist-cum-Questionnaire prepared (for the agreed scope of work) in the previous step.

C. Form Opinion on the Organization / Auditee meeting or not meeting to various security requirement and Generate Audit report in the Prescribed format.



Sample Security Audit Questionnaire

NC#	Control	Criteria
1	Audit Logging:	All journal entries include the following elements: a) date and time of the entry; b) serial or sequence number of entry (for automatic journal entries); c) kind of entry; d) source of entry (e.g., terminal, port, location, customer, etc.); and e) identity of the entity making the journal entry
2	Event Logged	The CA logs the following CA and subscriber (if applicable) key life cycle management related events: a. CA key generation; b. installation of manual cryptographic keys and its outcome (with the identity of the operator); c. CA key backup; d. CA key storage; e. CA key recovery; f. CA key escrow activities (if applicable); g. CA key usage; h. CA key archival; i. withdrawal of keying material from service; j. CA key destruction. k. CA key transportation; l. CA key migration m. identity of the entity authorising a key management operation; n. identity of the entities handling any keying material (such as key components or keys stored in portable devices or media); o. custody of keys and of devices or media holding keys; and p. compromise of a private key.

Sample Security Audit Questionnaire

NC #	Control	Criteria
3	Event Logged	The CA logs the following security-sensitive events: a. security-sensitive files or records read or written including the audit log itself; b. actions taken against security-sensitive data; c. security profile changes; d. use of identification and authentication mechanisms, both successful and unsuccessful (including multiple failed authentication attempts); e. system crashes, hardware failures and other anomalies; f. actions taken by individuals in Trusted Roles, computer operators, system administrators, and system security officers; g. change of affiliation of an entity; h. decisions to bypass encryption/authentication processes or procedures; and i. access to the CA system or any component thereof
4	Legal	The CA maintains controls and procedures to provide reasonable assurance that: • the CA and Root CA maintain the minimum levels of Commercial General Liability Insurance (occurrence form) and Professional Liability/Errors & Omissions insurance as established by the EV SSL Guidelines, and • the providers of the Insurance coverage meet the ratings qualifications established under the EV SSL Guidelines, or • If the CA and/or its root CA self-insures for liabilities, the CA and/or its root CA maintains the minimum liquid asset size requirement established in the EV SSL Guidelines.

AUDIT METHODOLOGY

Audit Encompasses:

- Risk Based assessment
- Use of Checklist Prepared based on the scope of audit, general IS Audit practices, guidelines issued by the CPA Canada Under the WebTrust Seal Program (WebTrust Program for Certification Authorities Guide. and the baseline requirements issued by the CAB Forum (CA-Brower Forum).
- Interviews with personnel / IT Staff / Functions / Process
- Observations & simulations of certain scenarios
- Following Globally accepted standards like ISMS/ISO 27001, BCM/ISO 22301, COBIT, Cyber Security Framework /CERT

WebTrust for CAs Seal

WebTrust Seal:

After completing the audit, a certificate authority is allowed to use the WebTrust seal to demonstrate that they have passed all items required by the WebTrust audit.

To obtain the WebTrust seal of assurance, the CA must meet all the WebTrust for Certification Authorities principles as measured by the WebTrust for Certification Authorities criteria associated with each of these principles

AUDIT CHALLENGES

Audit Experience as an Auditor (Not exhaustive, Audit still in Progress)

- It was rigorous, tough or challenging to understand the Web trust Principles, relate to the Controls practiced and already implemented by the CA. But doable.
- Understanding various very detailed both macro & micro level WebTrust security controls requirement & CAB Forum Baseline requirement, Observe, visualize/simulate certain scenarios, look for data points, assess/correlate the implementation strategy and look for evidence to complete the audit.
- Good part is that most of the controls of CCA audit checklist relating DSC, time stamping, and e-Sign either map to the WebTrust Principles or to the International Browser Forum Controls. Few Differences for e-Sign, DSC.
- PKI Guidelines of CCA like CCA-IOG, CCA-CP, CCA-IVG, CCA-TSG, CCA-SP, CCA-XMLSP, CCA-OCSP, CCA-SSL and Infrastructure Guidelines of CCA are embedded in one or the other Controls / standards specification of WebTrust

AUDIT REPORT FORMAT

REPORT OF THE INDEPENDENT ACCOUNTANT

- Scope
- Certification Authorities Responsibility
- Independent Accountant Responsibility
- Inherent Limitations
- Independent Accountant's Opinion
- Other Matters;
  - While the Auditee Firm assertion notes all issues disclosed on Bugzilla during the engagement period, we have only noted those instances relevant to the CAs enumerated in Attachment B and applicable to the WebTrust Principles and Criteria for Certification Authorities v2.2.

- **Use of the WebTrust Seal**

Auditee Firm's use of the WebTrust for Certification Authorities Seal constitutes a symbolic representation of the contents of this report, and it is not intended, nor should it be construed, to update this report to provide any additional assurance.

AUDIT REPORT FORMAT

REPORT OF THE INDEPENDENT ACCOUNTANT *contd.*

- Attachment A – Certificate Practice Statement, Certificate Policy Versions In-scope
- Attachment B – List of all CAs in Scope.
  - Root CA
  - Subordinate CAs
- Auditee Firm Management's Assertion
- Sample Report Format


Questions


Business Continuity

Partnering For Excellence

DIGITAL AGE STRATEGIES PVT. LTD.

Corporate Office:
 # 28, “Om Arcade”
2nd and 3rdFloors, Thimmappa Reddy Layout,
Hulimavu Gate, Bannerghatta Road
Bangalore 560 076
Ph: 91-080-26485148/41503825/41218560
Mobile: 94480 88666 / 94480 55711
Email: audit@digitalage.co.in
dinesh.shastri@digitalage.co.in