CERTIFICATION AUTHORITIES – EXTENDED VALIDATION AUDIT CRITERIA

Version 1.3

BASED ON:

CA/BROWSER FORUM

GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES

Version 1.3

TABLE OF CONTENTS

This document has been prepared for the use by those auditors recognized as eligible to perform EV audits by the CA/Browser Forum, Certification Authorities, Browsers and users of Extended Validation Certificates.

This document was prepared by the WebTrust Certification Authorities Advisory Group. Members of this Group are:

Chair	**Staff Contact:**
Donald E. Sheehy *Deloitte & Touche LLP* Michael Greene *Ernst & Young LLP* Mark Lundin *KPMG LLP* Jeffrey Ward *Stone Carlie & Company LLC*	Bryan Walker, *Canadian Institute of Chartered Accountants*

INTRODUCTION

1. The growth of internet transactions has emphasized the importance of strong authentication of the identity of web sites, domain owners and online servers. The Certificate Authorities ("CA") and browser developers have worked together to develop guidelines that create the basis for differentiating certificates which have stronger authentication standards than other certificates. Certificates that have been issued under stronger authentication controls, processes and procedures are called Extended Validation Certificates ("EV Certificates").

2. A working group known as the CA/Browser Forum consisting of many of the issuers of digital certificates and browser developers has developed a set of guidelines that set out the expected requirements for issuing EV certificates. The guidelines entitled "Guidelines for the Issuance and Management of Extended Validation Certificates" ("EV Guidelines") can be found at http://www.cabforum.org/.

3. CAs and browser developers have recognized the importance of an independent third party audit[1] of the controls, processes and procedures of CAs. Accordingly, the EV Guidelines include a specific requirement for CAs that wish to issue EV certificates.

4. The purpose of these EV Audit Criteria Guidelines is to set criteria that would be used as a basis for an auditor to conduct an EV audit.

Adoption

5. From April 1, 2008 until September 30, 2009 Version 1.1 of the Guidelines for the Issuance and Management of Extended Validation Certificates as published by the CA/Browser Forum was effective. Version 1.2 of the EV Guidelines became effective October 1, 2009. Version 1.3 of the EV Guidelines became effective November 20, 2010. These Audit Guidelines become applicable upon release.

6. The CA/Browser Forum may periodically publish errata that capture changes to the EV Guidelines. In addition the CA/Browser Forum will periodically modify the EV Guidelines to reflect more substantive changes in a point version (e.g., version 1.3). The auditor would need to consider only the updated approved version. The auditor is not required to consider the errata document.

[1] For the purposes of this document, the term "audit" has been used to describe an assurance engagement in which an auditor (practitioner) expresses a conclusion designed to enhance the degree of confidence on the intended users about the outcome of the evaluation against criteria. This is referred to as an "examination" in some jurisdictions.

TABLE 1 – EXAMPLE OF APPLICABLE VERSIONS OF THE EV CRITERIA		
Example Audit timeline	**EV Guidelines 1.**	**Current published version of the EV Guidelines (EV Guidelines 1.3 (Excluding the CA/Browser Forum's published Errata)**
Periods ending after September 30, 2009	1.2 (for the period prior to November 20, 2010	1.2 (For the period after November 20, 2010
Periods beginning and ending after November 20, 2010	Version 1.3	Version 1.3

7. As mentioned, the EV Audit Guidelines are to be used only in conjunction with an audit of the Certification Authority as required by the CA/Browser Forum Guidelines. The two audits would normally be conducted simultaneously. For CAs that have successfully (successfully meaning an opinion without reservation issued by an auditor) undergone a WebTrust for CA audit or ETSI TS102 042 v2.1.1 and the report is still current the procedures undertaken by the auditor would only be those that are necessary to examine the added criteria for EV certificates. The currently valid Certification Authorities audit would not need to be updated to a more recent date that would match the date of the EV audit.

8. If the CA does not have a currently valid WebTrust Seal of Assurance for CAs or an ETSI 102 042 audit, then before issuing EV Certificates, the CA and its Root CA must successfully complete either: (i) a point-in-time readiness assessment audit against the WebTrust for CA Program, and (ii) a point-in-time readiness assessment audit against the WebTrust EV Program, or an ETSI TS 102 042 V2.1.1. audit.

ADDENDUM Re Code Signing

Version 1.3 of the CA/Browser Forum's Guidelines for Extended Validation includes Guidelines with respect to Code Signing requirements. Included in these requirements is the necessity to have a WebTrust or ETSI examination. (See Appendix J, paragraph 6). No guidance with respect to this area is included in the attached Audit Criteria for Certification Authorities – Extended Validation Certificates Version 13.

CERTIFICATION AUTHORITIES – EXTENDED VALIDATION AUDIT CRITERIA

PRINCIPLE 1: **Certification Authority Extended Validation Business Practices Disclosure** - The Certification Authority (CA) discloses its Extended Validation (EV) Certificate practices and procedures and its commitment to provide EV Certificates in conformity with the applicable CA/Browser Forum Guidelines.

	EV Audit Criteria		
1	The CA and its Root CA discloses[2] on its website its: • EV Certificate practices, policies and procedures, • CAs in the hierarchy whose subject name is the same as the EV issuing CA, and • its commitment to conform to CA/Browser Forum Guidelines for Extended Validation Certificates. (See EV Certificate Guidelines Section 7.1.2)		
2	The Certificate Authority has published guidelines for revoking EV Certificates. (See EV Certificate Guidelines 11.2.1)		
3	The CA provides instructions to Subscribers, Relying Parties, Application Software Vendors and other third parties for reporting complaints or suspected private key compromise, EV Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to EV Certificates to the CA. (See EV Certificate Guidelines 11.3.1)		
4	The CA and its Root has controls to provide reasonable assurance that there is public access to the CPS on a 24x7 basis. The disclosures must be structured in accordance with either RFC 2527 or RFC 3647. (See EV Certificate Guidelines Section 7.1.2 (2))		

[2] The criteria are those that are to be tested for the purpose of expressing an opinion on WebTrust for Certificate Authorities - EV Audit Criteria. For an initial "readiness assessment" where there has not been a minimum of two months of operations disclosure to the public is not required. The CA, however, must have all other aspects of the disclosure completed such that the only action remaining is to activate the disclosure so that it can be accessed by users in accordance with the EV Guidelines.

PRINCIPLE 2: Service Integrity - The Certification Authority maintains effective controls to provide reasonable assurance that:

- EV Subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
- The integrity of keys and EV certificates it manages is established and protected throughout their life cycles.

	EV Audit Criteria		
	The following criteria apply to both new and renewed EV Certificates.		
	Subscriber Profile		
1.1	The CA maintains controls to provide reasonable assurance that it issues EV Certificates to Private Organizations, Government Entities, and Business Entities as defined within the EV Certificate Guidelines that meet the following requirements: For Private Organizations • the organization is a legally recognized entity whose existence was created by a filing with the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration or is an entity that is chartered by a state or federal regulatory agency; • the organization has designated with the Incorporating or Registration Agency either a Registered Agent, a Registered Office (as required under the laws of the jurisdiction of Incorporation or Registration), or an equivalent facility; • the organization is not designated as inactive, invalid, non-current or equivalent in records of the Incorporating Agency or Registration Agency; • the organization has a verifiable physical existence and business presence; • the organization's Jurisdiction of Incorporation, Registration, Charter, or License, and/or its Place of Business is not in a country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and • the organization is not listed on a published government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction. (See EV Certificate Guidelines Section 7.2.2) Or For Government Entities • the legal existence of the Government Entity is established by the political subdivision in which such Government Entity operates; • the Government Entity is not in a country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and • the Government Entity is not listed on a published government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.		

	EV Audit Criteria		
	(See EV Certificate Guidelines Section 7.2.3) Or For Business Entities • the entity is a legally recognized entity whose formation included the filing of certain forms with the Registration Agency in its Jurisdiction, the issuance or approval by such Registration Agency of a charter, certificate, or license, and whose existence can be verified with that Registration Agency; • the entity has a verifiable physical existence and business presence; • at least one Principal Individual associated with the business entity(owners, partners, managing members, directors or officers) is identified and validated; • the identified Principal Individual (owners, partners, managing members, directors or officers) attests to the representations made in the Subscriber agreement; • if the entity is represented under an assumed name, the legal existence and identity is verified in accordance with requirements of Section 10.3; • the entity or associated Principal Individual (owners, partners, managing members, directors or officers) is not located in a country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and • the entity or associated Principal Individual (owners, partners, managing members, directors or officers) is not listed on any published government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction. (See EV Certificate Guidelines Section 7.2.4)		
	Or For Non-commercial enterprises (International Organization Entities) • The Applicant is an International Organization Entity, created under a charter, treaty, convention or equivalent instrument that was signed by, or on behalf of, more than one country's government. and • The International Organization Entity is not be headquartered in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and • The International Organization Entity is not be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction. (See EV Certificate Guidelines Section 7.2.5)		

	EV Audit Criteria		
	EV CERTIFICATE CONTENT AND PROFILE		
2.1	The CA maintains controls to provide reasonable assurance that the EV certificates issued meet the minimum requirements for Certificate Content and profile as established in section 6 of the EV Certificate Guidelines including the following: • full legal organization name and if space is available the d/b/a name may also be disclosed • domain name • business Category • jurisdiction of Incorporation or Registration • registration Number • physical address of Place of Business. (See EV Certificate Guidelines Section 8)		
2.2	The CA maintains controls and procedures to provide reasonable assurance that the EV Certificates issued include the minimum requirements for the content of EV Certificates as established in the EV Certificate Guidelines relating to: • EV Subscriber Certificates • EV Subordinate CA Certificates. (See EV Certificate Guidelines Section 8.2)		
2.3	For EV Certificates issued to Subordinate CAs, the CA maintains controls and procedures to provide reasonable assurance that the certificates contain one or more OID that explicitly defines the EV Policies that Subordinate CA supports. (See EV Certificate Guidelines Section8.2.2)		
2.4	The CA maintains controls and procedures to provide reasonable assurance that EV Certificates are valid for a period not exceeding 27 months. (See EV Certificate Guidelines Section 8.3.1)		
2.5	The CA maintains controls and procedures to provide reasonable assurance that the data that supports the EV Certificates is revalidated within the time frames established in the EV Certificate Guidelines. (See EV Certificate Guidelines Section 8.3.2 and 13.3.2)		
	EV CERTIFICATE REQUEST REQUIREMENTS		

	EV Audit Criteria		
3	The CA maintains controls and procedures to provide reasonable assurance that the EV Certificate Request is: • obtained and complete prior to the issuance of EV Certificates (See EV Certificate Guidelines Section 9), • signed by an authorized individual (Certificate Requester), • properly certified as to being true and correct by the applicant, and • contains the information specified in Section 9 of the EV Certificate Guidelines.		
	Subscriber Agreement and Terms of Use		
4	The CA maintains controls and procedures to provide reasonable assurance that Subscriber Agreements: • are signed by an authorized Contract Signer, • names the applicant and the individual Contract Signer, and • contains provisions imposing obligations and warranties on the Application relating to - the accuracy of information - protection of Private Key - acceptance of EV Certificate - use of EV Certificate - reporting and revocation upon compromise - termination of use of EV Certificate. (See EV Certificate Guidelines Section 9.3)		
	INFORMATION VERIFICATION REQUIREMENTS		
	Verification of Applicant's Legal Existence and Identity		
5	The CA maintains controls and procedures to provide reasonable assurance that the following information provided by the Applicant is verified directly by performing the steps established by the EV Certificate Guidelines: Private Organization Subjects • legal Existence and Identity • legal Existence and Identity – Assumed Name • organization Name • registration Number		

	EV Audit Criteria		

	• registered agent
	Government Entity
	• legal Existence
	• entity Name
	• registration Number
	Business Entity
	• legal Existence
	• organization Name
	• registration Number
	• principle Individual.
	Non-Commercial Entity
	• International Organization Entities
	  • legal entities
	  • entity name
	  • registration number.
	(See EV Certificate Guidelines Sections 10.2 and 10.3))		

	Verification of Applicant		
6.1	The CA maintains controls and procedures to provide reasonable assurance that it verifies the physical address provided by Applicant is an address where Applicant conducts business operations (e.g., not a mail drop or P.O. box), and is the address of Applicant's Place of Business using a method of verification established by the EV Certificate Guidelines. (See EV Certificate Guidelines Section 10.4.1)		
6.2	The CA maintains controls and procedures to provide reasonable assurance that the telephone number provided by the Applicant is verified as a main phone number for Applicant's Place of Business by performing the steps set out in the EV Certificate Guidelines. (See EV Certificate Guidelines Section 10.4.2)		
6.3	If the Applicant has been in existence for less than three (3) years, as indicated by the records of the Incorporating Agency or Registration Agency, and is not listed in either the current version of one (1) Qualified Independent Information Source or a Qualified Governmental Tax Information Source, the CA maintains controls to provide reasonable assurance that the Applicant is actively engaged in business by: • verifying that the Applicant has an active current Demand Deposit Account with a		

	EV Audit Criteria		
	regulated financial institution, or • obtaining a Verified Legal Opinion or a Verified Accountant Letter that the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution. (See EV Certificate Guidelines Section 10.5)		
6.4	The CA maintains controls and procedures to provide reasonable assurance that the Applicant's registration or exclusive control of each domain name(s), to be listed in the EV Certificate, satisfies the following requirements using a method of verification established by the EV Certificate Guidelines: • the domain name is registered with an Internet Corporation for Assigned Names and Numbers (ICANN)-approved registrar or a registry listed by the Internet Assigned Numbers Authority (IANA). For Government Entity Applicants, the CA MAY rely on the domain name listed for that entity in the records of the QGIS in Applicant's Jurisdiction to verify Domain Name. • the Applicant: - is the registered holder of the domain name; or - has been granted the exclusive right to use the domain name by the registered holder of the domain name • the Applicant is aware of its registration or exclusive control of the domain name. • Registration information that is publicly available from the WHOIS database is compared with the verified Subject organization information and confirmed to be neither misleading nor inconsistent. (See EV Certificate Guidelines Section 10.6.1)		
	Verification of Other		
7.1	The CA maintains controls to provide reasonable assurance that it identifies "High Risk Applicants" and undertakes additional precautions as are reasonably necessary to ensure that such Applicants are properly verified using a verification method identified in the EV Certificate Guidelines. (See EV Certificate Guidelines Section 10.11.1)		
7.2	The CA maintains controls to provide reasonable assurance that no EV Certificate is issued if the Applicant, the Contract Signer, the Certificate Approver or the Applicant's Jurisdiction of Incorporation, Registration, or place of Business is: • on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the country of the CA's jurisdiction(s) of operation; or • has its Jurisdiction of Incorporation, or Registration, or Place of Business in any country with which the laws of the CA's jurisdiction prohibit doing business.		

	EV Audit Criteria		
	(See EV Certificate Guidelines Section 10.11.2)		
	Verification of Contract Signer and Approver		
8	The CA maintains controls and procedures to provide reasonable assurance that it verifies, using a method of verification established by the EV Certificate Guidelines: • the name and title of the Contract Signer and the Certificate Approver, as applicable and verifying that the Contract Signer and the Certificate Approver are agents representing the Applicant; • through a source other than the Contract Signer, that the Contract Signer is expressly authorized by the Applicant to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of the Applicant, including a contract that designates one or more Certificate Approvers on behalf of Applicant ("Signing Authority"); • through a source other than the Certificate Approver, that the Certificate Approver is expressly authorized by the Applicant to do the following, as of the date of the EV Certificate Request ("EV Authority") to: - submit, and if applicable authorize a Certificate Requester to submit, the EV Certificate Request on behalf of the Applicant; and - provide, and if applicable authorize a Certificate Requester to provide, the information requested from the Applicant by the CA for issuance of the EV Certificate; and - approve EV Certificate Requests submitted by a Certificate Requester. (See EV Certificate Guidelines Section 10.7)		
	Verification of EV Certificate requests		
9.1	The CA maintains controls to provide reasonable assurance, using a method of verification established in the EV Certificate Guidelines that: • subscriber Agreements are signed by an authorized Contract signer; • the EV Certificate Request is signed by the Certificate Requester submitting the document • if the Certificate requester is not also an authorized Certificate Approver, an authorized Certificate Approver independently approves the EV Certificate Request unless pre-authorized; and • signatures have been properly authenticated. (See EV Certificate Guidelines Section 10.8 and 10.9)		
9.2	In cases where an EV Certificate Request is submitted by a Certificate Requester, the CA maintains controls to provide reasonable assurance that, before it issues the requested EV Certificate, it verifies that an authorized Certificate Approver reviewed and approved the		

	EV Audit Criteria		
	EV Certificate Request. (See EV Certificate Guidelines Section 10.9)		
9.3	The CA maintains controls to provide reasonable assurance that it verifies information sources prior to placing reliance on them using a verification procedure set out in the EV Certificate Guidelines. The verification includes: • with respect to legal opinions; - the independent status of the author, - the basis of the opinion, and - authenticity. • with respect to accountants letters; - the independent status of the author, - the basis of the opinion, and - authenticity. • with respect to face-to-face vetting documents; - qualification of third-party validator, - document chain of custody, and - verification of attestation. • with respect to independent confirmation from applicant; - the request is initiated by the CA requesting verification of particular facts, - the request is directed to a Confirming Person at the Applicant or at the Applicant's Registered Agent or Registered Office using one of the acceptable methods stated by the CA/Browser Forum. - the Confirming Person confirms the fact or issue. • with respect to Qualified Independent Information Sources (QIIS) - the database used is a QIIS as defined by the EV Certificate Guidelines 10.10.5). • with respect to Qualified Government Information Sources (QGIS) - the database used is a QGIS as defined by the EV Certificate Guidelines 10.10.6. • with respect to Qualified Government Tax Information Source (QGTIS) - a Qualified Governmental information source is used that specifically contains tax information relating to Private Organizations, Business Entities or Individuals as defined by the EV Certificate Guidelines 10.10.7. (See EV Certificate Guidelines Section 10.10 and for Certificate Renewals Section 10.13)		

	EV Audit Criteria		
	Validation for Existing Subscribers (previously EV Certificate Renewal Verification Requirements)		
10.1	In conjunction with an EV Certificate Request placed by an Applicant who is already a customer of the CA, the CA MUST perform all authentication and verification tasks required by these Guidelines to ensure that the request is properly authorized by the Applicant and that the information in the EV Certificate will still be accurate and valid. (See EV Certificate Guidelines Section 10.13)		
	Other Matters		
11.1	Except for certificate requests approved by an Enterprise RA, the CA maintains controls to provide reasonable assurance that: • the set of information gathered to support a certificate request is reviewed for completeness and accuracy by an individual who did not gather such information; • any identified discrepancies are documented and resolved before certificate issuance; and • in the case where some or all of the documentation used to support the application is in a language other than the CA's normal operating language, the Final Cross-Correlation and Due Diligence is performed by employees under its control having appropriate training, experience, and judgment in confirming organizational identification and authorization and fulfilling all qualification requirements contained (See Section 29 of the EV Guidelines). When employees do not possess the language skills necessary to perform the Final Cross-Correlation and Due Diligence a CA may: - rely on the translations by a Translator or, if an RA is used, the CA must review the work completed by the RA and determine that all requirements have been met. - The CA may rely on the RA to perform the Final Cross-Correlation and Due Diligence, provided that the RA complies with Section 24 and is subjected to the Audit Requirements of Sections 14.1.2 and 14.1.3 as specified in the EV Guidelines. (See EV Certificate Guidelines Section 10.12, 12.1.3, 14.1)		
11.2	The CA maintains controls to provide reasonable assurance that RAs, subcontractors, and Enterprise RAs are contractually obligated to comply with the applicable requirements in the EV Certificate Guidelines and to perform them as required of the CA itself. (See EV Certificate Guidelines Section 12.2)		
	CERTIFICATE STATUS CHECKING AND REVOCATION		
12	The CA maintains controls to provide reasonable assurance that a repository is available 24x7 that enable Internet browsers to check online the current status of all certificates.		

	EV Audit Criteria		
	(See EV Certificate Guidelines Section 11.1)		
13	The CA maintains controls to provide reasonable assurance that: • for EV Certificates or Subordinate CA Certificates issued to entities not controlled by the entity that controls the Root CA - CRLs are updated and reissued at least every seven (7) days, and the nextUpdate field value is not more than ten (10) days, or - if the CA provides revocation of information via an Online Certificate Status Protocol (OCSP) service, the OCSP service is updated at least every four (4) days, and OCSP responses from this service MUST have a maximum expiration time of ten (10) days. • for subordinate CA Certificates controlled by the Root CA - CRLs are updated and reissued at least every twelve (12) months, and the nextUpdate field value is not more than twelve (12) months; or - if the CA provides revocation information via an Online Certificate Status Protocol (OCSP) service, the OCSP service is updated at least every twelve (12) months, and the OCSP responses from this service have a maximum expiration time of twelve (12) months. (See EV Certificate Guidelines Section 11.1.1)		
14	For CA that operate only a CRL capability, the CA maintains controls to provide reasonable assurance that an EV certificate chain can be downloaded in no more than 3 seconds over an analog telephone line under normal network conditions. (See EV Certificate Guidelines Section 11.1.2)		
15	The CA performs capacity planning at least annually to operate and maintain its CRL or OCSP to provide commercially reasonable response times. (See EV Certificate Guidelines Section 11.1.3)		
16	The CA maintains controls to provide reasonable assurance that Revocation procedures established in the EV Certificate Guidelines are followed.		
17	The CA maintains controls to provide reasonable assurance that Revocation entries on a CRL or OCSP are not removed until after the expiration date of the revoked EV Certificate. (See EV Certificate Guidelines Section 11.1.4)		
18	The CA maintains controls to provide reasonable assurance that it can accept and respond to revocation requests and related inquiries on a continuous 24x7 basis. (See EV Certificate Guidelines Section 11.2.1)		
19	The CA maintains controls to provide reasonable assurance that EV Certificates are		

	EV Audit Criteria		
	revoked on the occurrence of any of the following events: • the Subscriber requests revocation of its EV Certificate; • the Subscriber indicates that the original EV Certificate Request was not authorized and does not retroactively grant authorization; • the CA obtains reasonable evidence that the Subscriber's private key (corresponding to the public key in the EV Certificate) has been compromised, or that the EV Certificate has otherwise been misused; • the CA receives notice or otherwise becomes aware that a Subscriber has violated any obligation under the Subscriber Agreement deemed material by the CA: • the CA receives notice or otherwise become aware that a court or arbitrator has revoked a Subscriber's right to use the domain name listed in the EV Certificate, or that the Subscriber has failed to renew it domain name; • the CA receives notice or otherwise becomes aware of a material change in the information contained in the EV Certificate; • a determination, in the CA's sole discretion, that the EV Certificate was not issued in accordance with the terms and conditions of these Guidelines or the CA's EV Policies; • the CA determines that any of the information appearing in the EV Certificate is not accurate. • the CA ceases operations for any reason and has not arranged for another EV CA to provide revocation support for the EV Certificate; • the CA's right to issue EV Certificates under these Guidelines expires or is revoked or terminated unless the CA makes arrangements to continue maintaining the CRL/OCSP Repository; • the CA's Private Key of the CA's Root Certificate used for issuing that EV Certificate is suspected to have been compromised; • such additional revocation events as the CA publishes in its EV Policies; • the CA receives notice or otherwise becomes aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of the CA's jurisdiction of operation as described in Section 23 of the EV Certificate Guidelines. (See EV Certificate Guidelines Section 11.2.2 and Section 10.1.1)		
20	The CA maintains controls to provide reasonable assurance that it: • has the capability to accept and acknowledge Certificate Problem Reports on a 24x7 basis; • identifies high priority Certificate Problem Reports; • begin investigation of Certificate Problem Reports within 24 hours:		

	EV Audit Criteria		
	• decides whether revocation or other appropriate action is warranted; and • where appropriate, forwards such complaints to law enforcement. (See EV Certificate Guidelines Section 11.3.2 and Section 11.3.3)		
21	The CA maintains controls to provide reasonable assurance that ensure the system used to process and approve EV Certificate Requests requires actions by at least two trusted persons before the EV Certificate is created. (See EV Certificate Guidelines Section 13.3.4)		
22	The CA maintains controls to provide reasonable assurance that: • it performs ongoing self audits against a randomly selected sample of at least three percent (3%) of the EV Certificates issued. For all EV Certificates where the final cross correlation and due diligence requirements of Section 24 of the EV Guidelines are performed by an RA, this sample size is increased to six (6%) percent. • for new root keys generated after November 11, 2006 for the purpose of issuing EV Certificates, the CA obtained an unqualified report from the CA's qualified auditor opining on the CA's root key and certificate generation process. (See EV Certificate Guidelines Section 14.1.2 and 14.1.5)		
23	The CA maintains controls and procedures to provide reasonable assurance that: • applicable requirements of the CA/Browser Forum Guidelines for Extended Validation Certificates are included (directly or by reference) in contracts with subordinate CAs, RAs, Enterprise RAs, and subcontractors that involve or relate to the issuance or maintenance of EV Certificates, and • the CA monitors and enforces compliance with the terms of the contracts. (See EV Certificate Guidelines Section 7.1.2(3))		
24	The CA maintains controls to provide reasonable assurance that it complies with: • laws applicable to its business and the certificates it issues in each jurisdiction where it operates, and • licensing requirements in each jurisdiction where it issues EV certificates. (See EV Certificate Guidelines Section 7.1.1)		
25	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 Certificate Guidelines, and • the providers of the Insurance coverage meet the ratings qualifications established under the EV Certificate Guidelines, or • If the CA and/or its root CA self insures for liabilities, the CA and/or its root CA		

	EV Audit Criteria		
	maintains the minimum liquid asset size requirement established in the EV Certificate Guidelines. (See EV Certificate Guidelines Section 7.1.3)		
	EMPLOYEE AND THIRD PARTY ISSUES		
26.1	With respect to employees, agents, or independent contractors engaged in the EV process, the CA maintains controls to: • verify the identity of each person, • perform background checks of such person to confirm employment, check personal references, confirm the highest or most relevant educational degree obtained and search criminal records where allowed in the jurisdiction where the person will be employed, and • for employees at the time of the adoption of the EV Certificate Guidelines by the CA verify the identity and perform background checks within three months of the date of the adoption of the EV Certificate Guidelines. (See EV Certificate Guidelines Section 12.1.1)		
26.2	The CA maintains controls to provide reasonable assurance that: • all personnel performing validation duties (Validation Specialists) have been trained with skill training that covers basic public key infrastructure (PKI) knowledge, authentication and verification policies and procedures, common threats to the validation process including phishing and other social engineering tactics, and these Guidelines; • records of such training are maintained; • personnel entrusted with Validation Specialist duties meet a minimum skills requirement that enables them to perform such duties satisfactorily; • validation Specialists engaged in EV Certificate issuance are qualified to have issuance privilege, consistent with a CA's training and performance programs; • validation Specialists qualify for each skill level required by the corresponding validation task before granting privilege to perform said task; • validation Specialists take and pass an audit on the EV Certificate validation criteria outlined in these Guidelines. (See EV Certificate Guidelines Section 12.1.2)		
27	The CA maintains controls to provide reasonable assurance that there is a separation of duties such that no one person can both validate and authorize the issuance of an EV Certificate. (See EV Certificate Guidelines Section 12.1.3)		

	EV Audit Criteria		
	DATA AND RECORD ISSUES		
28	The CA maintains controls to provide reasonable assurance that the following EV key and certificate management events are recorded and maintained and the records maintained: • CA key lifecycle management events, including: - key generation, backup, storage, recovery, archival, and destruction - cryptographic device lifecycle management events. • CA and Subscriber EV Certificate lifecycle management events, including: - EV Certificate Requests, renewal and re-key requests, and revocation - all verification activities required by these Guidelines - date, time, phone number used, persons spoken to, and end results of verification telephone calls - acceptance and rejection of EV Certificate Requests - issuance of EV Certificates - generation of EV Certificate revocation lists (CRLs) and OCSP entries. • the CA maintains controls to provide reasonable assurance that following security events are recorded: - successful and unsuccessful PKI system access attempts - PKI and security system actions performed - security profile changes - system crashes, hardware failures, and other anomalies - firewall and router activities - entries to and exits from CA facility. • Log entries MUST include the following elements: - Date and time of entry - Identity of the person making the journal entry - Description of entry (See EV Certificate Guidelines Section 13.1)		
29	The CA and RA maintain controls to provide reasonable assurance that event logs at the CA and RA site are retained for at least seven years. (See EV Certificate Guidelines Section 13.2.1)		
30	The CA maintains controls to provide reasonable assurance that all previously revoked certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns are recorded in an internally managed database and used to		

	EV Audit Criteria		
	flag suspicious EV Certificate Requests. (See EV Certificate Guidelines Section 13.2.2)		
31	The CA has a policy to retain all documentation relating to all EV Certificate Requests and verification thereof, and all EV Certificates and revocation thereof, for at least seven years after any EV Certificate based on that documentation ceases to be valid. (See EV Certificate Guidelines Section13.2.2)		
32	The CA maintains controls to provide reasonable assurance that risks impacting its CA operations over EV certifications are assessed regularly and address the following: • identify reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any EV Data or EV Processes; • assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the EV Data and EV Processes; and • assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to control such risks. (See EV Certificate Guidelines Section 13.3.2 and Section 3)		
33	The CA develops, implement, and maintain a Security Plan consisting of security, policies, procedures, measures, and products designed to reasonably manage and control the risks identified during the Risk Assessment. (See EV Certificate Guidelines Section 13.3.3)		

Appendix A

CA/BROWSER FORUM

GUIDELINES FOR
EXTENDED VALIDATION CERTIFICATES

To download a copy of the current CA/Browser Forum EV SSL Certificate Guidelines Version 1.3 go to:

http://www.cabforum.org/documents.html