WEBTRUST® FOR CERTIFICATION AUTHORITIES

WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES – SSL BASELINE WITH NETWORK SECURITY

Version 2.3

Release Date 1 February 2018

Effective Date For audit periods commencing on or after 1 February 2018

Based on the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates – Version 1.5.4, and Network and Certificate Systems Security Requirements – Version 1.1.

Document History

Version	Publication Date	Revision Summary
2.0	3 April 2014	Updated SSL Baseline Audit Criteria to conform to SSL Baseline Requirements v1.1.6 and incorporate Network and Certificate Systems Security Requirements v1.0 into the Audit Criteria as Principle 4
2.1	1 November 2016	Updated SSL Baseline Audit Criteria to conform to SSL Baseline Requirements v1.4.1, including remapping all criteria reference numbers as the SSL Baseline Requirements were updated to conform to RFC 3647. Additionally, the following changes were made: • Principle 1, Criterion 6 – Updated disclosure requirements for CAA Records • Principle 1, Criterion 7 – Requirement for CP/CPS to include CA contact information • Principle 1, Criterion 8 – Requirement for CA to ensure public repository is read-only • Principle 2, Criterion 1.1 – Clarified language and included Subordinate CA Key Pairs in scope. • Principle 2, Criteria Section 2.x – Reorganised to provide better clarity, including adding criterion for certificate serial number entropy (2.1), the SHA-1 sunset (2.10), and an explicit requirement of certificate conformance to RFC 5280 (2.6). • Principle 2, Criterion 2.1.4 – Updated to add subject:givenName and subject:surname. • Principle 2, Criterion 3.3 – Added language to include Subordinate CA Private Keys and allowing the CA to archive the Subscriber or Subordinate CA Private Key if the Subscriber or Subordinate CA authorises it • Principle 2, Criterion 4.1 – Updated to include requirements for wildcard domain validation and new gTLDs (generic top-level domains) • Principle 2, Criterion 4.6 – Updated BR reference • Principle 2, Criterion 4.11 – Minor language updates • Principle 2, Criterion 5.1 – Added language that the CA must maintain a process for subscribers to request revocations of their own certificates • Principle 2, Criterion 5.3 – Minor language updates • Principle 2, Criterion 5.5 – Updated language to include explicit references to revocation information being made available via cRLDistributionPoints and authorityInformationAccess certificate extensions. • Principle 2, Criterion 5.9 – Updated RFC2560 to RFC6960 • Principle 2, Criterion 6.2 – Updated language to include the requirement that all personnel in Trusted Roles are required to maintain skill levels consistent with the CA's training and

		performance programs. Previously, this read Validation Specialists. • Principle 2, Criterion 6.7 – Updated language to refer to the requirements as stipulated in Section 1.3.2 of the BRs • Principle 2, Criterion 7.3 – Minor language updates • Principle 2, Criteria Section 8.x – Split 8.1 to two criteria (8.1 and 8.2) for clarity, renumbered 8.2-8.4 to 8.3-8.5. Minor language updates to 8.3 (formerly 8.2) • Principle 3 – Minor language updates • Principle 3, Criterion 11 – Clarified that it is the CA private key • Principle 3, Criterion 12 – Moved multi-factor authentication requirement to its own criterion (from criterion 5) • Principle 4 – Split into individual criteria and minor language updates
2.2	31 January 2017	Updated SSL Baseline Audit Criteria to conform to SSL Baseline Requirements v1.4.2 • Updated the applicability of SSL Baseline Requirements Section 3.2.2.4 and Appendix D.
2.3	1 February 2018	Updated SSL Baseline Audit Criteria to conform to SSL Baseline Requirements v1.5.4 and Network and Certificate System Security Requirements v1.1 • Principle 1, Criterion 6 – Require CAs to disclose their CAA Records policy in their CPS • Principle 2, Criterion 2.14 – Clarified the requirement for Root and Subordinate CA Subject Information • Principle 2, Criterion 4.1 – Updated that domain validation must be completed prior to issuance (instead as of the time of issuance), and that the CA maintains a record of the domain validation method (and associated BR version number) used. • Principle 2, Criterion 4.6 – Revised age of data from 39 months to 825 days for certificates issued on or after 1 March 2018, and updated to reflect re-use of previously completed validations • Principle 2, Criterion 4.10 and 4.11 – New criteria added to address CAA Records processing requirements. • Principle 2, Criterion 4.12 and 4.13 – Renumbered from 4.10 and 4.11. • Principle 2, Criterion 8.3 – Updated that this criterion is only effective for certificates issued before 11 August 2017 • Principle 4 – Updates made to conform to CA/B Forum Ballot 210

Acknowledgements

This document has been prepared by the WebTrust/PKI Assurance Task Force (the "Task Force") for use by those auditors licensed to perform WebTrust for Certification Authorities audits by CPA Canada.

Members of the Task Force are:

- Jeffrey Ward, *BDO USA, LLP* (Chair)
- Donald E. Sheehy (Vice-Chair)
- Chris Czajczyc, *Deloitte LLP*
- Reema Anand, *KPMG LLP*
- David Roque, *Ernst & Young LLP*

Significant support has been provided by:

- Daniel J. Adam, *Deloitte & Touche LLP*
- Donoghue Clarke, *Ernst & Young LLP*
- Timothy Crawford, *BDO USA, LLP*
- Zain Shabbir, *KPMG LLP*

CPA Canada Support

- Kaylynn Pippo, (Staff Contact)
- Bryan Walker, Consultant
- Janet Treasure, Vice President, Member Development and Support
- Gord Beal, Vice President, Research, Guidance and Support

Table of Contents

Introduction

The primary goal of the CA/Browser Forum's ("Forum") Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements", "SSL Baseline Requirements" or "BRs") and Network and Certificate Systems Security Requirements ("Network Security Requirements") is to enable efficient and secure electronic communication, whilst addressing user concerns about the trustworthiness of Certificates. The Requirements also serve to inform users and help them to make informed decisions when relying on Certificates.

The CA/Browser Forum, that consists of many of the issuers of digital certificates and browser and other application developers, has developed guidelines that set out the expected requirements for issuing SSL[1] certificates (the "Baseline Requirements").

The Forum has also issued additional security guidelines (the "Network and Certificate System Security Requirements") that apply to all publicly trusted Certification Authorities (CAs), regardless of certificate type being issued.

The purpose of these WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security ("Audit Criteria") is to set out criteria that would be used as a basis for an auditor to conduct a SSL Baseline Requirements and Network and Certificate Systems Security Requirements audit.

Adoption and effective dates

These Audit Criteria incorporate and make reference to relevant CA/Browser Forum Guidelines and Requirements as listed in Appendix A, and are effective for audit periods commencing on or after 1 February 2018.

The Forum may periodically publish updated Guidelines and Requirements. The auditor is generally not required to consider these updated versions until reflected in the subsequently updated Audit Criteria. However, in certain circumstances whereby a previous requirement or guidelines is eliminated or made less restrictive, the auditor may consider those changes as of their effective dates even if the changes are not reflected in the most current Audit Criteria.

In certain instances, the Forum updates its Guidelines and Requirements with certain criteria only effective at a date later than the publication date. The auditor is directed to review the document history, revisions, and relevant dates in the Forum documents to understand the applicability of certain Guidelines and Requirements.

For a list of Forum Guidelines and Requirements that have effective dates later than the effective date of these Audit Criteria, as well as other nuances, refer to Appendix D.

Additionally, auditors should be aware that Browsers may impose additional requirements, above and beyond the CA/Browser Forum Guidelines and Requirements that would be outside of the scope of an engagement performed in accordance with WebTrust Principles and Criteria for Certification

[1] The term SSL is used to refer to certificates intended to authenticate servers, based on the original SSL protocol which was used. Modern browser and application deployments make use of newer technologies such as TLS, and are equally in scope for these requirements.

Authorities – SSL Baseline with Network Security. The auditor is encouraged to make such enquiries of the CA to determine whether any additional procedures should be performed and related reporting undertaken to satisfy the relevant Browser(s). When such additional procedures are required outside of the scope of the WebTrust criteria specified herein, auditors should also consider the appropriate reporting to be issued to the Browser(s) to satisfy their requirements.

Connection with WebTrust for CA

These Audit Criteria are designed to be used in conjunction with an audit of a CA as required by the CA/Browser Forum. Due to significant overlap between these Audit Criteria and the WebTrust Principles and Criteria for Certification Authorities Version 2.x or later ("WebTrust for CA" or "WTCA"), this audit should be conducted simultaneously with the WebTrust for CA audit.

Requirements not subject to audit

In preparing these Audit Criteria, the Task Force reviewed the relevant CA/Browser Forum documents as outlined in Appendix A, with the intent of identifying items that would not be subject to audit. The results of this review are set out in Appendix B and Appendix C.

Audit scoping

As of the time of publication, these SSL Baseline with Network Security audit criteria incorporate two different CA/Browser Forum requirements documents:

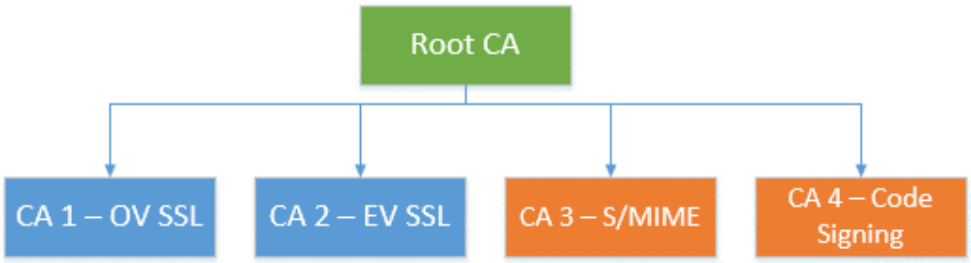
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("SSL Baseline Requirements"); and
- Network and Certificate System Security Requirements ("Network Security Requirements")

The SSL Baseline Requirements are addressed in Principles 1, 2, and 3 of these audit criteria. The Network Security Requirements are addressed in Principle 4 of these audit criteria.

The SSL Baseline Requirements only apply to PKI hierarchies (root and subordinate CAs) that issue or are capable of issuing publicly trusted SSL/TLS certificates intended to authenticate servers on the Internet (i.e. certificates containing the id_kp_serverAuth OID (1.3.6.1.5.5.7.3.1) and/or the anyExtendedKeyUsage OID (2.5.29.37.0) in the extKeyUsage extension).

The Network Security Requirements apply to all CAs within a publicly trusted PKI hierarchy, even if those certificates are designed for other uses (i.e. code signing, client authentication, secure email, document signing etc.).

For example, in the following PKI hierarchy:



The SSL Baseline Requirements (Principles 1, 2, and 3) would only apply to Root CA, CA 1, and CA 2 (provided CA 3 and CA 4 are technically constrained and are not capable of issuing SSL/TLS certificates). However, the Network Security Requirements (Principle 4) would apply to all CAs – Root CA, CA 1, CA 2, CA 3, and CA 4.

The auditor is directed to consider the above when determining which criteria are in scope for which CAs in a given hierarchy under audit.

Principle 1: SSL Baseline Requirements Business Practices Disclosure

The Certification Authority (CA) discloses its SSL Certificate practices and procedures and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Requirements.

#	Criterion	Ref[2]
1	The CA discloses[3] on its website: • SSL Certificate practices, policies and procedures; • Cross Certificates that identify the CA as the Subject, provided that the CA arranged for or accepted the establishment of the trust relationship (i.e. the Cross Certificate at issue); and • its commitment to conform to the latest version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum.	2.2, 3.2.6
2	The CA discloses in the Certificate Policy (CP) and/or Certification Practice Statement (CPS) that it includes its limitations on liability, if the CA chooses to limit its liability for Certificates that are not issued or managed in compliance with these Requirements or its Certificate Policy and/or Certification Practice Statement.	9.8
3	The Issuing CA documents in its CP or CPS that the Certificates it issues containing the specified policy identifier(s) are managed in accordance with the SSL Baseline Requirements.	7.1.6
4	The Certificate Authority has controls to provide reasonable assurance that the CA CP and/or CPS that describes how the CA implements the latest version of the Baseline Requirements are updated annually.	2.0, 2.3
5	The CA and its Root has controls to provide reasonable assurance that there is public access to the CP and/or CPS on a 24x7 basis, and the content and structure of the CP and/or CPS are in accordance with either RFC 2527 or RFC 3647.	2
6	The CA discloses in its Certificate Policy (CP) and/or Certification Practices Statement (CPS) under section 4.2 (if the CA's disclosures follow RFC 3647) or under section 4.1 (if the CA's disclosures follow RFC 2527) its policy or practice on processing CAA (Certification Authority Authorisation) DNS Records for Fully Qualified Domain Names	2.2

[2] Reference to the applicable section(s) of the SSL Baseline Requirements for this criterion. The auditor is directed to consider the referenced section(s) as part of assessing the CA's compliance with each criterion

[3] The criteria are those that are to be tested for the purpose of expressing an opinion on Trust Services Principles and Criteria for Certification Authorities – SSL Baseline with Network Security. 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 SSL Baseline Requirements.

	that is consistent with the SSL Baseline Requirements, and specifies the set of Issuer Domain Names that that the CA recognises in CAA "issue" or "issuewild" records as permitting it to issue. The CA maintains controls to provide reasonable assurance that it logs all actions taken, if any, consistent with its processing practice.	
7	Effective as of 3 December 2016, the CA's CP/CPS provides a link to a web page or an email address for contacting the person or persons responsible for operation of the CA.	1.5.2
8	Effective as of 3 December 2016, the CA has controls to provide reasonable assurance that public access to its repository is read-only.	2.4

Principle 2: SSL Service Integrity

The Certification Authority (CA) maintains effective controls to provide reasonable assurance that:

- 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 certificates it manages is established and protected throughout their life cycles.

#	Criterion	Ref[4]
	KEY GENERATION CEREMONIES	
1.1	The CA maintains controls to provide reasonable assurance that Root CA and Subordinate CA Key Pairs are created in accordance with SSL Baseline Requirements Section 6.1.1.1.	6.1.1.1
	CERTIFICATE CONTENT AND PROFILE	
2.1	The CA maintains controls to provide reasonable assurance that Root, Subordinate, and Subscriber certificates generated by the CA contain certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.	7.1
2.2	The CA maintains controls to provide reasonable assurance that the version of certificates issued are of type x.509 v3.	7.1.1
2.3	The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Root CA certificates generated conform to the Baseline Requirements.	7.1.2.1, 6.1.5, 7.1.6, 7.1.6.2
2.4	The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Subordinate CA certificates conform to the Baseline Requirements.	7.1.2.2, 6.1.5, 7.1.6, 7.1.6.3
2.5	The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Subscriber certificates generated conform to the Baseline Requirements.	7.1.2.3, 6.1.5, 7.1.6, 7.1.6.4
2.6	The CA maintains controls to provide reasonable assurance that with exception to the requirements stipulated in the Baseline Requirements Sections 7.1.2.1,	7.1.2.4

[4] Reference to the applicable section(s) of the SSL Baseline Requirements for this criterion. The auditor is directed to consider the referenced section(s) as part of assessing the CA's compliance with each criterion

	7.1.2.2, and 7.1.2.3, all other fields and extensions of certificates generated are set in accordance with RFC 5280.	
2.7	The CA maintains controls to provide reasonable assurance that the validity period of Subscriber certificates issued does not exceed the maximum as specified in the Baseline Requirements.	6.3.2
2.8	The CA maintains controls to provide reasonable assurance that it does not issue certificates with extensions that do not apply in the context of the public Internet, unless: a. Such values fall within an OID arc for which the Applicant demonstrates ownership; or b. The Applicant can otherwise demonstrate the right to assert the data in public context	7.1.2.4
2.9	The CA maintains controls to provide reasonable assurance that it does not issue certificates with semantics that, if included, will mislead a Relying Party about the certificate information verified by the CA	7.1.2.4
2.10	The CA maintains controls to provide reasonable assurance that it does not issue any new Subscriber or Subordinate CA certificates using the SHA-1 hash algorithm.	7.1.3
2.11	The CA maintains controls to provide reasonable assurance that the content of the Certificate Issuer Distinguished Name field matches the Subject DN of the Issuing CA to support name chaining as specified in RFC 5280, section 4.1.2.4.	7.1.4.1
2.12	The CA maintains controls to provide reasonable assurance that for Subscriber certificates issued: • The subjectAltName extension is present and contains at least one entry • Each entry MUST be either: o A dNSName containing the Fully-Qualified Domain Name (Wildcard FQDNs permitted); or o An iPAddress containing the IP address of a server.	7.1.4.2.1
2.13	The CA maintains controls to provide reasonable assurance that it does not issue certificates containing a Reserved IP Address or Internal Name in the subjectAltName extension or subject:commonName field, and as of 1 October 2016, will revoke any certificate containing a Reserved IP Address or Internal Name.	7.1.4.2.1
2.14	The CA maintains controls to provide reasonable assurance that Subject information of Certificates conforms to the Baseline Requirements, including: • subject:commonName • subject:organizationName • subject:givenName • subject:surname • subject:streetAddress • subject:localityName • subject:stateOrProvinceName • subject:postalCode • subject:countryName	7.1.4.2.2, 7.1.6, 7.1.4.3

	• subject:organizationalUnitName • Other Subject Attributes • Subject field requirements if Reserved Certificate Policy Identifiers are asserted • Subject Information for Root and Subordinate CA certificates	
2.15	The CA maintains controls to provide reasonable assurance that Subordinate CA certificates technically constrained using the nameConstraints extension conform to the Baseline Requirements.	7.1.5
2.16	The CA maintains controls to provide reasonable assurance that it rejects a certificate request if the Public Key does not meet the requirements set forth in Sections 6.1.5, 6.1.6, or if it has a weak Private Key (such as a Debian weak key).	6.1.1.3, 6.1.5, 6.1.6
	CERTIFICATE REQUEST REQUIREMENTS	
3.1	The CA maintains controls to provide reasonable assurance that the CA, prior to the issuance of a Certificate obtains the following documentation from the Applicant: 1. A certificate request, which may be electronic; 2. An executed Subscriber or Terms of Use Agreement, which may be electronic; and 3. Any additional documentation the CA determines necessary to meet the Baseline Requirements.	4.1.2
3.2	The CA maintains controls to provide reasonable assurance that the Certificate Request is: • obtained and complete prior to the issuance of Certificates; • signed by an authorized individual (Certificate Requester); • properly certified as to being correct by the applicant; and • contains the information specified in Section 4.2.1 of the SSL Baseline Requirements.	4.1.2, 4.2.1
	Subscriber and Subordinate CA Private Keys	
3.3	The CA maintains controls to provide reasonable assurance that it does not archive the Subscriber or Subordinate CA Private Keys. Additionally: • If the CA or any of its designated RAs generated the Private Key on behalf of the Subscriber or Subordinate CA, then the CA shall encrypt the Private Key for transport to the Subscriber or Subordinate CA. • If the CA or any of its designated RAs become aware that a Subscriber's or Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber or Subordinate CA, then the CA shall revoke all certificates that include the Public Key corresponding to the communicated Private Key. • The CA only archives a Subscriber or Subordinate CA Private Key if it receives authorisation from the Subscriber or Subordinate CA.	6.1.2, 6.2.5, 6.2.6

	Subscriber Agreements and Terms of Use	
3.4	The CA maintains controls to provide reasonable assurance that the CA, prior to the issuance of a Certificate, obtains a Subscriber and/or Terms of Use agreement in accordance with the SSL Baseline Requirements Section 9.6.3. That agreement contains provisions imposing obligations and warranties on the Application relating to: • the accuracy of information • protection of Private Key • acceptance of certificate • use of certificate • reporting and revocation • termination of use of certificate • responsiveness • acknowledgement and acceptance.	9.6.3
	VERIFICATION PRACTICES	
	Verification of Domain Control	
4.1	The CA maintains controls to provide reasonable assurance that prior to issuing a Certificate: • the CA obtains confirmation in accordance with the SSL Baseline Requirements Sections 3.2.2.4, 3.2.2.5, 3.2.2.6 and 4.2.2 related to the Fully-Qualified Domain Name(s) (including wildcard domains and new gTLDs (generic top-level domains)) and IP address(es) listed in the Certificate; and • the CA maintains records of which validation method, including the relevant SSL Baseline Requirements version number, used to validate every domain.	3.2.2.4, 3.2.2.5, 3.2.2.6, 4.2.2
	Verification of Subject Identity Information	
4.2	The CA maintains controls to provide reasonable assurance that the following information provided by the Applicant is verified directly by performing the steps established by the SSL Baseline Requirements: • Identity (SSL Baseline Requirements Section 3.2.2.1) • DBA/Trade name (SSL Baseline Requirements Section 3.2.2.2) • Authenticity of Certificate Request (SSL Baseline Requirements Section 3.2.5) • Verification of Individual Applicant (SSL Baseline Requirements Section 3.2.3) • Verification of Country (SSL Baseline Requirements Section 3.2.2.3)	3.2.2.1, 3.2.2.2, 3.2.5, 3.2.3, 3.2.2.3
4.3	The CA maintains controls to provide reasonable assurance that it inspects any document relied upon for identity confirmation for alteration or falsification.	3.2.2
4.4	The CA maintains controls to provide reasonable assurance that it allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then the CA SHALL NOT accept any certificate requests that are outside this specification. The	3.2.5

	CA SHALL provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.	
4.5	The CA maintains controls to provide reasonable assurance that it screens proxy servers in order to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located, when the subjectcountryName field is present.	3.2.2.3
4.6	The CA maintains controls to provide reasonable assurance that the CA does not use any data or document from a source specified under Section 3.2 of SSL Baseline Requirements to validate a certificate request, or re-use a previously completed validation conducted by itself, if the data or document was obtained, or validation completed more than: a) 39 months prior to issuing the certificate if the certificate is issued prior to 1 March 2018; and b) 825 days prior to issuing the certificate if the certificate is issued on or after 1 March 2018.	4.2.1
4.7	The CA maintains controls to provide reasonable assurance that the CA uses an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns to identify subsequent suspicious certificate requests.	4.1.1
4.8	The CA maintains controls to provide reasonable assurance that the CA identifies high risk certificate requests, and conducts additional verification activities in accordance with the SSL Baseline Requirements.	4.2.1
4.9	The CA maintains controls to provide reasonable assurance that, prior to using a data source, the CA evaluates the data source's accuracy and reliability in accordance with the requirements set forth in Section 3.2.2.7 of the SSL Baseline Requirements.	3.2.2.7
4.10	For certificates issued on or after 8 September 2017, the CA maintains controls to provide reasonable assurance that as part of the issuance process, it checks for CAA records, and, if present, processes the certificate request in accordance with the requirements set forth in Section 3.2.2.8 of the Baseline Requirements.	3.2.2.8
4.11	The CA maintains controls to provide reasonable assurance that it documents potential certificate issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CA/Browser Forum on the circumstances.	3.2.2.8
Certificate Issuance by a Root CA		
4.12	The CA maintains controls to provide reasonable assurance that Certificate issuance by the Root CA shall require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.	4.3.1

4.13	The CA maintains controls to provide reasonable assurance that Root CA Private Keys are not used to sign certificates, except as stipulated in the Baseline Requirements.	6.1.7
	CERTIFICATE REVOCATION AND STATUS CHECKING	
5.1	The CA maintains controls to provide reasonable assurance that a process is available 24x7 that the CA is able to accept and respond to revocation requests and related inquiries, and that the CA provides a process for Subscribers to request revocation of their own certificates.	4.9.3
5.2	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: • decides whether revocation or other appropriate action is warranted; and • where appropriate, forwards such complaints to law enforcement.	4.9.3, 4.9.5, 4.10.2
5.3	The CA maintains controls to provide reasonable assurance that Subscriber Certificates are revoked within 24 hours if any of the following events occurs: 1. The Subscriber requests in writing that the CA revoke the Certificate; 2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization; 3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of SSL Baseline Requirements Sections 6.1.5 and 6.1.6; 4. The CA obtains evidence that the Certificate was misused; 5. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use; 6. The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name); 7. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name; 8. The CA is made aware of a material change in the information contained in the Certificate; 9. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement; 10. The CA determines that any of the information appearing in the Certificate is inaccurate or misleading; 11. The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;	4.9.1.2, 6.1.5, 6.1.6

	12. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository; 13. The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate; 14. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or 15. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).	
5.4	The CA maintains controls to provide reasonable assurance that Subordinate CA Certificates are revoked within 7 days if any of the following events occurs: 1. The Subordinate CA requests revocation in writing; 2. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization; 3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of SSL Baseline Requirements Sections 6.1.5 and 6.1.6, 4. The Issuing CA obtains evidence that the Certificate was misused; 5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with these Baseline Requirements or the applicable Certificate Policy or Certification Practice Statement; 6. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading; 7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate; 8. The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; 9. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement; or 10. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk.	4.9.1.2, 6.1.5, 6.1.6
5.5	The CA maintains controls to provide reasonable assurance that the CA: • makes revocation information available via the cRLDistributionPoints and/or authorityInformationAccess certificate extensions for Subordinate CA and Subscriber Certificates in accordance with the SSL Baseline Requirements Section 7.1.2. • for high-traffic FQDNs, distributes its OCSP responses in accordance with SSL Baseline Requirements.	7.1.2, 4.9.11

5.6	The CA maintains controls to provide reasonable assurance that an online 24x7 Repository is provided that application software can use to automatically check the current status of all unexpired Certificates issued by the CA, and: • for the status of Subscriber Certificates: o If the CA publishes a CRL, then the CA shall update and reissue CRLs at least once every seven (7) days, and the value of the nextUpdate field must not be more than ten (10) days beyond the value of the thisUpdate field; and o The CA shall update information provided via an Online Certificate Status Protocol (OCSP) at least every four (4) days and OCSP responses must have a maximum expiration time of ten (10) days. • for the status of subordinate CA Certificates o The CA shall update and reissue CRLs at least (i) once every twelve (12) months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field must not be more than twelve months beyond the value of the thisUpdate field; and o The CA shall update information provided via an Online Certificate Status Protocol at least (i) every twelve (12) months and (ii) within 24 hours after revoking a Subordinate CA Certificate. • The CA makes revocation information available through an OCSP capability using the GET method for Certificates issued in accordance with the SSL Baseline Requirements.	4.10.2, 4.9.7, 4.9.10
5.7	The CA maintains controls to provide reasonable assurance that the CA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.	4.10.2
5.8	The CA maintains controls to provide reasonable assurance that the CA does not remove revocation entries on a CRL or OCSP Response until after the Expiry Date of the revoked Certificate.	4.10.1
5.9	The CA maintains controls to provide reasonable assurance that OCSP responses conform to RFC6960 and/or RFC5019, and are signed either: • by the CA that issued the Certificates whose revocation status is being checked, or • by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked (the OCSP signing Certificate must contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960).	4.9.9
5.10	The CA maintains controls to provide reasonable assurance that OCSP responses by CA's which have not been technically constrained in accordance with SSL Baseline Requirements Section 7.1.5 do not respond with a "good" status for Certificates that have not been issued.	4.9.10
EMPLOYEES AND THIRD PARTIES		

6.1	The CA maintains controls to verify the identity and trustworthiness of an employee, agent, or independent contractor prior to engagement of such persons in the Certificate Management Process.	5.3.1
6.2	The CA maintains controls to provide reasonable assurance that: • the CA provides all personnel performing information verification duties (Validation Specialists) with skills-training that covers basic Public Key Infrastructure (PKI) knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements. • the CA maintains records of such training and ensures that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily. • the CA documents each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task. • the CA requires all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the Baseline Requirements. • all personnel in Trusted Roles maintain skill levels consistent with the CA's training and performance programs.	5.3.3, 5.3.4
6.3	The CA maintains controls to provide reasonable assurance that before the CA authorizes a Delegated Third Party to perform a delegated function, the CA contractually require the Delegated party to: • meet the qualification requirements of the Baseline Requirements Section 5.3.1, when applicable to the delegated function; • retain documentation in accordance with the Baseline Requirements Section 5.5.2; • abide by the other provisions of the Baseline Requirements that are applicable to the delegated function; and • comply with (a) the CA's Certificate Policy/Certification Practice Statement or (b) the Delegated Third Party's practice statement that the CA has verified complies with these Requirements.	1.3.2, 5.3.1, 5.5.2
6.4	The CA maintains controls to provide reasonable assurance that the CA verifies that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 5.3.3 and the document retention and event logging requirements of Section 5.4.1.	5.3.7, 5.3.3, 5.4.1
6.5	For High Risk Certificate Requests, the CA maintains controls to provide reasonable assurance that the CA verifies that the Delegated Third Party's processes to identify and further verify High Risk Certificate Requests meets the requirements of the CA's own processes for High Risk Certificate Requests.	4.2.1
6.6	The CA maintains controls to provide reasonable assurance that the CA internally audits each Delegated Third Party's compliance with the Baseline Requirements on an annual basis.	8.7

6.7	The CA maintains controls to provide reasonable assurance that the CA does not accept certificate requests authorized by an Enterprise RA unless the requirements in SSL Baseline Requirements Section 1.3.2 are met, and the CA imposes these requirements on the Enterprise RA, and monitors compliance by the Enterprise RA.	1.3.2
	DATA RECORDS	
7.1	The CA maintains controls to provide reasonable assurance that the CA records details of the actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved.	5.4.1

7.2	The CA maintains controls to provide reasonable assurance that the following events are recorded:
	
	• CA key lifecycle management events, including:
	  o key generation, backup, storage, recovery, archival, and destruction
	  o cryptographic device lifecycle management events.
	• CA and Subscriber Certificate lifecycle management events, including:
	  o Certificate Requests, renewal and re-key requests, and revocation
	  o all verification activities stipulated in the Baseline Requirements and the CA's Certification Practice Statement
	  o date, time, phone number used, persons spoken to, and end results of verification telephone calls
	  o acceptance and rejection of certificate requests
	  o issuance of Certificates
	  o generation of Certificate Revocation Lists (CRLs) and OCSP entries.
	• security events, including:
	  o successful and unsuccessful PKI system access attempts
	  o PKI and security system actions performed
	  o security profile changes
	  o system crashes, hardware failures, and other anomalies
	  o firewall and router activities
	  o entries to and exits from CA facility.
	• Log entries must include the following elements:
	  o Date and time of entry
	  o Identity of the person making the journal entry
	  o Description of entry
		5.4.1

7.3	The CA maintains controls to provide reasonable assurance that audit logs generated are retained for at least seven years.	5.4.3
7.4	The CA maintains controls to provide reasonable assurance that all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, is retained for at least seven years after any Certificate based on that documentation ceases to be valid.	5.5.2
	AUDIT	

8.1	The CA maintains controls to provide reasonable assurance that for Subordinate CAs that are considered technically constrained in accordance with SSL Baseline Requirements Section 7.1.5, the CA: • monitors the Subordinate CA's adherence to the CA's Certificate Policy and the Subordinate CA's Certification Practices Statement; and • performs quarterly assessments against a randomly selected sample of at least three percent (3%) of the Certificates issued by the Subordinate CA in the period beginning immediately after the last samples was taken to ensure all applicable Baseline Requirements are met.	8.1, 8.7, 7.1.5
8.2	The CA maintains controls to provide reasonable assurance that for Subordinate CAs that are NOT considered technically constrained in accordance with SSL Baseline Requirements Section 7.1.5, the CA verifies that Subordinate CAs that are not technically constrained are audited in accordance with SSL Baseline Requirements 8.4.	8.1, 8.4, 7.1.5
8.3	For certificates issued before 11 August 2017, the CA maintains controls to provide reasonable assurance that if the CA uses a Delegated Third Party that is not an Enterprise and is not currently audited, prior the certificate issuance, the CA ensures the domain control validation process required under SSL Baseline Requirements Section 3.2.2.4 or IP address verification under Section 3.2.2.5 has been performed by the Delegated Third Party by either: • using an out-of-band mechanism involving at least one human who is acting on either on behalf of the CA or on behalf of the Delegated Third Party to confirm the authenticity of the certificate request or the information supporting the certificate request; or • performing the domain control validation process itself.	8.4, 3.2.2.4, 3.2.2.5
8.4	The CA maintains controls to provide reasonable assurance that: • it performs ongoing self-assessments on at least a quarterly basis against a randomly selected sample of at least three percent (3%) of the Certificates issued during the period commencing immediately after the previous self-assessment samples was taken, • Except for Delegated Third Parties that undergo an annual audit that meets the criteria specified in the Baseline Requirements, the CA performs ongoing quarterly assessments against a randomly selected sample of at least three percent (3%) of the Certificates verified by the Delegated Third Party in the period beginning immediately after the last samples was taken • The CA reviews each Delegated Third Party's practices and procedures to assess that the Delegated Third Party is in compliance with these Requirements and the relevant Certificate Policy and/or Certification Practice Statement.	8.7
8.5	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 SSL certificates.	8.0

Principle 3: CA Environmental Security

The Certification Authority (CA) maintains effective controls to provide reasonable assurance that:

- Logical and physical access to CA systems and data is restricted to authorized individuals;
- The continuity of key and certificate management operations is maintained; and
- CA systems development, maintenance and operations are properly authorized and performed to maintain CA systems integrity.

#	Criterion	Ref[5]
1	The CA maintains controls to provide reasonable assurance that it develops, implements, and maintains a comprehensive security program designed to: • protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes; • protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes; • protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes; • protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and • comply with all other security requirements applicable to the CA by law.	5.0
2	The CA maintains controls to provide reasonable assurance that it performs a risk assessment at least annually which: • Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes; • Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and • Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.	5.0, 5.4.8
3	The CA maintains controls to provide reasonable assurance that it develops, implements, and maintains a Security Plan consisting of security procedures, measures, and products designed to reasonably manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan:	5.0

[5] Reference to the applicable section(s) of the SSL Baseline Requirements for this criterion. The auditor is directed to consider the referenced section(s) as part of assessing the CA's compliance with each criterion

	• includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. • takes into account then-available technology and the cost of implementing the specific measures, and • is designed to implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.	
4	The CA maintains controls to provide reasonable assurance that it develops, implements, and maintains a Business Continuity Plan that includes at a minimum: • the conditions for activating the plan; • emergency procedures; • fall-back procedures; • resumption procedures; • a maintenance schedule for the plan; • awareness and education requirements; • the responsibilities of the individuals; • recovery time objective (RTO); • regular testing of contingency plans; • the CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes; • a requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location; • what constitutes an acceptable system outage and recovery time; • how frequently backup copies of essential business information and software are taken; • the distance of recovery facilities to the CA's main site; and • procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site. The Business Continuity Plan is tested at least annually, reviewed, and updated.[6]	5.7.1
5	The CA maintains controls to provide reasonable assurance that its Certificate Management Process includes: • physical security and environmental controls (see WTCA 2.0 Section 3.4); • system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention (see WTCA 2.0 Section 3.7); • network security and firewall management, including port restrictions and IP address filtering (see WTCA 2.0 Section 3.6);	5.0

[6] For organizations that are undergoing a WebTrust for CA audit (examination), all of the above are required and already tested with the exception of the disclosure of the distance of recovery facilities to the CA's main site.

	• user management, separate trusted-role assignments, education, awareness, and training (see WTCA 2.0 Section 3.3); and • logical access controls, activity logging, and inactivity time-outs to provide individual accountability (see WTCA 2.0 Section 3.6).	
6	The CA maintains controls to provide reasonable assurance that: • physical access to CA facilities and equipment is limited to authorized individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control; • CA facilities and equipment are protected from environmental hazards; • loss, damage or compromise of assets and interruption to business activities are prevented; and • compromise of information and information processing facilities is prevented.	5.0 (WTCA v2.0 Sec 3.4)
7	The CA maintains controls to provide reasonable assurance that CA systems development and maintenance activities are documented, tested, authorized, and properly implemented to maintain CA system integrity.	5.0 (WTCA v2.0 Sec 3.7)
8	The CA maintains controls to provide reasonable assurance that CA system access is limited to authorized individuals. Such controls provide reasonable assurance that: • operating system and database access is limited to authorized individuals with predetermined task privileges; • access to network segments housing CA systems is limited to authorized individuals, applications and services; and • CA application use is limited to authorized individuals. Such controls must include, but are not limited to: • network security and firewall management, including port restrictions and IP address filtering; • logical access controls, activity logging (WTCA 2.0 Section 3.10), and inactivity time-outs to provide individual accountability.	5.0 (WTCA v2.0 Sec 3.6)
9	The CA maintains controls to provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations.	5.0 (WTCA v2.0 Sec 3.3)
10	The CA maintains controls to provide reasonable assurance that: • significant CA environmental, key management, and certificate management events are accurately and appropriately logged; • the confidentiality and integrity of current and archived audit logs are maintained; • audit logs are completely and confidentially archived in accordance with disclosed business practices; and	5.0 (WTCA v2.0 Sec 3.10)

	• audit logs are reviewed periodically by authorized personnel	
11	The CA maintains controls to provide reasonable assurance that: • CA private keys are protected in a system or device that has been validated as meeting at least FIPS 140[-2] level 3 or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats; • CA private keys outside the validated system or device specified above are protected with physical security, encryption, or a combination of both in a manner that prevents disclosure of the private keys; • CA private keys are encrypted with an algorithm and key-length that meets current strength requirements (2048-bit minimum); • CA private keys are backed up, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment; and • physical and logical safeguards to prevent unauthorized certificate issuance.	5.2.2, 6.2, 6.2.7
12	The CA maintains controls to provide reasonable assurance that it enforces multi-factor authentication for all accounts capable of directly causing certificate issuance.	6.5.1

Principle 4: Network and Certificate System Security Requirements

The Certification Authority (CA) maintains effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum.

#	Criterion	Ref[7]
	GENERAL PROTECTIONS FOR THE NETWORK AND SUPPORTING SYSTEMS	
1.1	The CA maintains controls to provide reasonable assurance that certificate Systems are segmented into networks based on their functional, or logical relationship.	1.a
1.2	The CA maintains controls to provide reasonable assurance that equivalent security controls for Certificate Systems apply to all systems co-located in the same network.	1.b
1.3	The CA maintains controls to provide reasonable assurance that Root CA Systems are located in a High Security Zone and in an offline state or air-gapped from all other networks.	1.c
1.4	The CA maintains controls to provide reasonable assurance that Issuing Systems, Certificate Management Systems, and Security Support Systems are maintained and protected in at least a Secure Zone.	1.d
1.5	The CA maintains controls to provide reasonable assurance that Security Support Systems are implemented and configured to protect systems and communications between systems inside Secure Zones and High Security Zones, and communications with non-Certificate Systems outside those zones (including those with organizational business units that do not provide PKI-related services) and those on public networks.	1.e
1.6	The CA maintains controls to provide reasonable assurance that networks are configured with rules that support only the services, protocols, ports, and communications that the CA has identified as necessary to its operations.	1.f
1.7	The CA maintains controls to provide reasonable assurance that Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems are configured by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's or Delegated Third Party's operations and allowing only those that are approved by the CA or Delegated Third Party.	1.g

[7] Reference to the applicable section(s) of the Network and Certificate System Security Requirements.

1.8	The CA maintains controls to provide reasonable assurance that configurations of Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems are reviewed on at least a weekly basis to determine whether any changes violated the CA's security policies.	1.h
1.9	The CA maintains controls to provide reasonable assurance that administration access to Certificate Systems is granted only to persons acting in Trusted Roles and require their accountability for the Certificate System's security.	1.i
1.10	The CA maintains controls to provide reasonable assurance that multi-factor authentication is implemented to each component of the Certificate System that supports it.	1.j
1.11	The CA maintain controls to provide reasonable assurance that authentication keys and passwords for any privileged account or service account on a Certificate System are changed, when a person's authorization to administratively access that account on the Certificate System is changed or revoked.	1.k
1.12	The CA maintains controls to provide reasonable assurance that recommended security patches are applied to Certificate Systems within six (6) months of the security patch's availability, unless the CA documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.	1.l
TRUSTED ROLES, DELEGATED THIRD PARTIES, AND SYSTEM ACCOUNTS		
2.1	The CA maintains controls to provide reasonable assurance that a documented procedure for appointing individuals to Trusted Roles and assigning responsibilities to them is followed.	2.a
2.2	The CA maintains controls to provide reasonable assurance that the responsibilities and tasks assigned to Trusted Roles are documented and "separation of duties" for such Trusted Roles based on the risk assessment of the functions to be performed is implemented.	2.b
2.3	The CA maintains controls to provide reasonable assurance that only personnel assigned to Trusted Roles have access to Secure Zones and High Security Zones.	2.c
2.4	The CA maintains controls to provide reasonable assurance that individuals in a Trusted Role act only within the scope of such role when performing administrative tasks assigned to that role.	2.d
2.5	The CA maintains controls to provide reasonable assurance that employees and contractors observe the principle of "least privilege" when accessing, or when configuring access privileges on, Certificate Systems.	2.e
2.6	The CA maintains controls to provide reasonable assurance that Trusted Roles use a unique credential created by or assigned to that person for authentication to Certificate Systems.	2.f

2.7	The CA maintains controls to provide reasonable assurance that Trusted Roles using a username and password to authenticate shall configure accounts to include but not be limited to:
	
	• For accounts accessible only within Secure Zones or High Security Zones:
	  o Passwords have at least twelve (12) characters for accounts not publicly accessible
	• For accounts accessible from outside a Secure Zone or High Security Zone:
	  o Passwords to have at least eight (8) characters, be changed at least every three (3) months, use a combination of at least numeric and alphabetic characters, not be one of the user's previous four (4) passwords; and implement account lockout for failed access attempts; OR
	  o Implement a documented password management and account lockout policy that the CA has determined provide at least the same amount of protection against password guessing as the foregoing controls.
		2.g

2.8	The CA maintains controls to provide reasonable assurance that Trusted Roles log out of or lock workstations when no longer in use.	2.h
2.9	The CA maintains controls to provide reasonable assurance that workstations are configured with inactivity time-outs that log the user off or lock the workstation after a set time of inactivity without input from the user.	2.i
2.10	The CA maintains controls to provide reasonable assurance that it reviews all system accounts at least every three (3) months and deactivates any accounts that are no longer necessary for operations.	2.j
2.11	The CA maintains controls to provide reasonable assurance that it revokes account access to Certificate Systems after no more than five (5) failed access attempts, provided that this security measure is supported by the Certificate System and does not weaken the security of this authentication control.	2.k
2.12	The CA maintains controls to provide reasonable assurance that it disables all privileged access of an individual to Certificate Systems within twenty-four (24) hours upon termination of the individual's employment or contracting relationship with the CA or Delegated Third Party.	2.l
2.13	The CA maintains controls to provide reasonable assurance that it enforces multi-factor OR multi-party authentication for administrator access to Issuing Systems and Certificate Management Systems.	2.m
2.14	The CA maintains controls to provide reasonable assurance that each Delegated Third Party shall be: • Required to use multi-factor authentication prior to the Delegated Third Party approving issuance of a Certificate; OR • Be technically constrained that restrict the Delegated Third Party's ability to approve certificate issuance for a limited set of domain names.	2.n

2.15	The CA maintains controls to provide reasonable assurance that it restricts remote administration or access to an Issuing System, Certificate Management System, or Security Support System except when: • The remote connection originates from a device owned or controlled by the CA or Delegated Third Party; • The remote connection is through a temporary, non-persistent encrypted channel that is supported by multi-factor authentication; and • The remote connection is made to a designated intermediary device meeting the following: o Located within the CA's network; o Secured in accordance with the Network and Certificate System Security Requirements; and o Mediates the remote connection to the Issuing System.	2.o
LOGGING, MONITORING, AND ALERTING		
3.1	The CA maintains controls to provide reasonable assurance that Security Support Systems under the control of CA or Delegated Third Party Trusted Roles are implemented to monitor, detect, and report any security-related configuration change to Certificate Systems.	3.a
3.2	The CA maintains controls to provide reasonable assurance that Certificate Systems under the control of CA or Delegated Third Party Trusted Roles capable of monitoring and logging system activity are configured to continuously monitor and log system activity.	3.b
3.3	The CA maintains controls to provide reasonable assurance that Automated mechanisms under the control of CA or Delegated Third Party Trusted Roles are configured to process logged system activity and alert personnel, using notices provided to multiple destinations, of possible Critical Security Events.	3.c
3.4	The CA maintains controls to provide reasonable assurance that Trusted Role personnel follows up on alerts of possible Critical Security Events.	3.d
3.5	The CA maintains controls to provide reasonable assurance that a human review of application and system logs is performed at least monthly and includes: • Validating the integrity of logging processes; and • Testing the monitoring, logging, alerting, and log-integrity-verification functions are operating properly.	3.e
3.6	The CA maintains controls to provide reasonable assurance that it maintains, archives, and retains logs in accordance with its disclosed business practices.	3.f
VULNERABILITY DETECTION AND PATCH MANAGEMENT		
4.1	The CA maintains controls to provide reasonable assurance that intrusion detection and prevention controls under the control of CA or Delegated Third Party Trusted Roles are implemented to protect Certificate Systems against common network and system threats.	4.a

4.2	The CA maintains controls to provide reasonable assurance that a formal documented vulnerability correction process is followed and includes identification, review, response, and remediation of vulnerabilities.	4.b
4.3	The CA maintains controls to provide reasonable assurance that a Vulnerability Scan is performed on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems based on the following: • Within one (1) week of receiving a request from the CA/Browser Forum; • After any system or network changes that the CA determines are significant; and • At least every three (3) months	4.c
4.4	The CA maintains controls to provide reasonable assurance that a Penetration Test is performed on the CA's and each Delegated Third Party's Certificate Systems on at least an annual basis and after infrastructure or application upgrades or modifications that the CA determines are significant.	4.d
4.5	The CA maintains controls to provide reasonable assurance that it documents that Vulnerability Scans and Penetrations Tests were performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test.	4.e
4.6	The CA maintains controls to provide reasonable assurance that it performs one of the following within ninety-six (96) hours of discovery of a Critical Vulnerability not previously addressed by the CA's vulnerability correction process: • Remediate the Critical Vulnerability; • If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to the following: o Vulnerabilities with high CVSS scores, starting with the vulnerabilities the CA determines are the most critical (such as those with a CVSS score of 10.0); and o Systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; OR • Document the factual basis for the CA's determination that the vulnerability does not require remediation because of one of the following: o The CA disagrees with the NVD rating; o The identification is a false positive; o The exploit of the vulnerability is prevented by compensating controls or an absence of threats; or o Other similar reasons.	4.f

Appendix A: CA/Browser Forum Documents

These Audit Criteria are based on the following CA/Browser Forum Documents:

Document Name	Version	Effective Date
Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates	1.5.4	4 October 2017
Network and Certificate System Security Requirements	1.1	1 October 2017

Copies of these documents are available on the CA/Browser Forum's website at:

https://cabforum.org/documents

Appendix B: Sections of SSL Baseline Requirements not subject to audit

Sections of the Baseline Requirements which contain no content or the phrase 'No Stipulation' were not considered for audit. Additionally, the following items are not subject to audit:

Ref	Topic	Reasons for exclusion
1.1	Overview	Information only, no auditable items
1.2	Document Name and Identification	Information only, no auditable items
1.3 (except 1.3.2)	PKI Participants	Information only, no auditable items
1.4	Certificate Usage	Information only, no auditable items
1.5 (except 1.5.2)	Policy Administration	Information only, no auditable items
1.6	Definitions and Acronyms	No auditable items, however the auditor is directed to consider these definitions when interpreting the SSL Baseline Requirements and these audit criteria.
4.9.2	Who Can Request Revocation	Information only, auditable items are covered in other criteria
8.2	Identity/Qualifications of Assessor	Information only, no auditable items
8.6	Communication of Results	Information only, no auditable items
9.6.1	CA Representations and Warranties	Legal item
9.9.1	Indemnification by CAs	Legal item
9.16.3	Severability	Legal item

Appendix C: Sections of Network and Certificate System Security Requirements not subject to audit

Ref	Topic	Reasons for exclusion
2.g.ii	Password controls, specifically the portion of the requirement which reads: 'not a dictionary word or on a list of previously disclosed human-generated passwords'.	Items would require disclosures of user passwords or rainbow table scans of the password hash values.

Appendix D: CA/Browser Forum effective date differences

SSL Baseline Requirements

The following Baseline Requirements have effective dates later than the effective date of these Audit Criteria. Refer to details and instructions below for guidance on how to address these as part of an audit:

Ref	Effective Date	Guidance
1.5.2	3 December 2016	The requirements specified in this section need only be considered as of 3 December 2016 onwards.
2.3	3 December 2016	The requirements specified in this section need only be considered as of 3 December 2016 onwards.
2.4	3 December 2016	The requirements specified in this section need only be considered as of 3 December 2016 onwards.
3.2.2.4	7 January 2017	Baseline Requirements v1.3.8 replaced the entirety of the domain validation requirements in this section with new requirements. These were subsequently amended again in v1.4.2. For certificates issued on or before 6 January 2017, the auditor is directed to consider the domain validation requirements in Section 3.2.2.4 of Baseline Requirements v1.3.6. For certificates issued on or after 7 January 2017, the auditor is directed to consider the domain validation requirements in Section 3.2.2.4 of Baseline Requirements v1.4.2. NOTE: Additional amendments to Section 3.2.2.4 are likely in 2017 and the auditor is encouraged to check subsequent versions of the Baseline Requirements and the effective dates of any amendments to this section.
6.3.2	1 March 2018	The maximum validity of certificates issued on or after 1 March 2018 must not exceed 825 days. For certificates issued prior to 1 March 2018 but on or after 1 July 2016, the validity period must not exceed 39 months.
7.1.4.3	8 June 2017	For Root and Subordinate CA certificates issued on or after 8 June 2017, the Common Name field in the certificate subject must be present. Prior to 8 June 2017, the Common Name field was optional.