CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Webtrust® for Certification Authorities

WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES – VERIFIED MARK CERTIFICATES

Release Date 1 December 2021

Effective Date For engagement periods commencing on or after 1 December 2021

Based on the Minimum Security Requirements for the Issuance of Verified Mark Certificate Guidelines – Version 1.0

Document History

Version	Publication Date	Revision Summary
1.0	1 December 2021	Initial release.

Acknowledgements

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

Members of the Task Force are:

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

Significant support has been provided by:

- Timothy Crawford, *BDO USA, LLP*
- Daniel J. Adam, *Deloitte & Touche LLP*
- Donoghue Clarke, *Ernst & Young LLP*
- Eric Lin, *Ernst & Young LLP*

Canada Support

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

Table of Contents

Introduction

Introduction to WebTrust Principles and Criteria for Verified Mark Certificates Version 1.0

The purpose of these WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates ("Criteria") is to set out principles and criteria that would be used by a practitioner to conduct a Verified Mark Certificate assurance engagement based on the Verified Mark Certificate Requirements (VMCR) v 1.4 issued by the Authindicators Working Group, a voluntary organization that maintains the VMC Requirements.

The primary goal of these requirements is to describe an integrated set of technologies, protocols, and identity and mark proofing requirements that are necessary for the issuance and management of Verified Mark Certificates (VMCs) – certificates that are trusted by Consuming Entities and Relying Parties. Version 1.4 of the VMCR can be found at https://bimigroup.org/resources/VMC_Guidelines_latest.pdf.

Relevant sections of the VMCRs have been synchronized with the following versions of the CA/Browser Forum standards (at https://cabforum.org):

- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v1.7.0 ("Baseline Requirements")
- Guidelines For The Issuance And Management Of Extended Validation Certificates v1.7.2

The CA/Browser Forum may periodically publish updated Guidelines and Requirements. The VMCRs will not incorporate the updates, unless specifically referenced in updated versions of the VMCRs.

Upon adoption, these criteria are mandatory for Certification Authorities ("CA") who issue or plan to issue VMCs.

Verified Mark Certificate Overview

VMCs assert a cryptographically verifiable and auditable binding between an identity, a logo, and a domain. The key pair of an end entity VMC is unused, and there are no requirements around the generation, storage, and protection of such key pairs. In particular, CAs may generate such key pairs on behalf of their customers, and VMCs need not be revoked if the unused key pair is compromised.

VMCs present Consuming Entities and Relying Parties with information about and marks asserted by the Mark Asserting Entity (also referred to as subscriber(s) or VMC subscriber(s)), some of which is gathered from legal documents and government registries (including trademark registries). When Mark Verifying Authorities verify marks presented by a Mark Asserting Entity for inclusion in a VMC, or when Mark Verifying Authorities present VMCs and the information or marks they contain to Consuming Entities, or when Consuming Entities present VMCs and the information or marks they contain to Relying Parties, they are not providing legal advice to any party.

Adoption and effective dates

These Criteria incorporate and refer to the VMCR v 1.4. These WebTrust Principles and Criteria for Certification Authorities – Verified Mark Criteria are effective for audit periods commencing on or after 1 December 2021. s. Earlier adoption is permitted and encouraged.

The VMCR may also be updated from time to time and the practitioner is not required to consider these updated versions until reflected in the subsequently updated WebTrust Criteria. The practitioner is directed to review the current version of the VMCR history, revisions, and relevant dates to understand the applicability of certain Guidelines and Requirements.

Connection with WebTrust for Certification Authorities

These Criteria are designed to be used in conjunction with a WebTrust Principles and Criteria for Certification Authorities Version 2.2 or later assurance engagement of r ("WTCA") as required by the VMCR. Due to significant overlap between these Criteria and those for WTCA engagements, this VMC engagement should be conducted simultaneously with the WTCA engagement. These criteria have significant overlap with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security ("WTBR") and WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL ("WTEV SSL"). While these criteria have significant overlap and can be conducted simultaneously, the practitioner should evaluate and report on how controls impact each hierarchy separately.

Network and Certificate System Security Requirements

Principle 4 of these Criteria is based on the CA/Browser Forum's Network and Certificate Systems Security Requirements (NCSSR), Version 1.7, dated April 5, 2021. The NCSSRs are subject to changes more frequently than these criteria and practitioners should ensure they are considering the most recent versions of the NCSSR.

Guidelines for the Issuance and Management of Extended Validation Certificates

Principle 2 of these Criteria refer to the CA/Browser Forum's Guidelines for the Issuance and Management of Extended Validation, Version 1.7.5 (GL EV), dated April 5, 2021, detailing the certificate profile requirements and validation requirements, along with the requirements in the VMCR. The GL EV are subject to changes more frequently than these Criteria and practitioners should ensure they are considering the most recent version of the GL EV.

Requirements not subject to Assurance

In preparing these Criteria, the Task Force reviewed the relevant VMCR with the intent of identifying items that would not be subject to assurance. The results of this review are set out in Appendix B.

Principle 1: Policy Management and Business Practices Disclosure

The Certification Authority (CA) discloses its VMC practices and procedures and its commitment to provide VMCs in conformity with the applicable VMCR.

#	Criterion	VMCRRef[1]
1.1	The CA discloses on its website its Certificate Policy (CP) and/or Certification Practice Statement (CPS).	2.2
1.2	The CA 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 and include all material required by RFC 3647.	2.2
1.3	The CA discloses in section 4.2 of its Certificate Policy (CP) and/or Certification Practices Statement (CPS) its policy or practice on processing CAA (Certification Authority Authorisation) Domain Name System (DNS) Records for Fully Qualified Domain Names that is consistent with the VMCR, and specifies the set of Issuer Domain Names that that the CA The CA maintains controls to provide reasonable assurance that it logs all actions taken, if any, consistent with its processing practice. recognises in CAA “issue” or “issuevmc” records as permitting it to issue.	2.2
1.4	The Certificate Authority has controls to provide reasonable assurance that the CA CP and/or CPS that describe how the CA implements the latest version of the VMCR are updated annually.	2.3
1.5	The CA discloses in the CP and/or CPS any 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 CP and/or CPS.	9.8
1.6	The CA’s CP and/or 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
1.7	The CA has controls to provide reasonable assurance that public access to its repository is read-only.	2.4
1.8	The CA discloses all Cross Certificates that identify the CA as the Subject in accordance with the VMCR, Section 3.2.19.	3.2.19

1 Reference to the applicable section(s) of the Verified Mark Certificate Requirements v 1.0 for this criterion. The practitioner is directed to consider the referenced section(s) as part of assessing the CA’s compliance with each criterion.

Principle 2: VMC Service Integrity

The CA maintains effective controls to provide reasonable assurance that:

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

Key generation ceremonies

#	Criterion	VMCRRef
1.1	The CA maintains controls to provide reasonable assurance that Root CA and Subordinate CA Key Pairs are created in accordance with VMCR Section 6.1.1.1.	6.1.1.1

VMC subscriber and certificate content profile

Subscriber profile and verification of subject information

#	Criterion	VMCRRef
2.1	The CA maintains controls to provide reasonable assurance that it issues VMCs to Private Organizations as defined within the VMCR that meet the following requirements: • the organization is a legally recognized entity whose existence was created or recognized by a filing with (or an act of) the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration (e.g., by issuance of a certificate of incorporation registration number, etc.) or created or recognized by a Government Agency (e.g., under a charter, treaty, convention, or equivalent recognition instrument); • the entity designated with the Incorporating or Registration Agency, a Registered Agent, or a Registered Office (as required under the laws of the jurisdiction of Incorporation or Registration), or an equivalent facility; • the entity is not designated as inactive, invalid, non-current or equivalent on the records of the Incorporating Agency or Registration Agency;	3.2.2.1

#	Criterion	VMCRRef
2.1 *(cont'd)*	• the entity has a verifiable physical existence and business presence; • the entity'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 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.	
2.2	The CA maintains controls to provide reasonable assurance that it issues VMC to Government Entities as defined within the VMCR that meet the following requirements: • the entity's legal existence was established by the political subdivision in which the entity operates; • the 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 entity is not listed on a government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.	3.2.2.2
2.3	The CA maintains controls to provide reasonable assurance that it issues VMC to Business Entities, defined within the VMCR as applicants that meet the following requirements: • the entity is a legally recognized entity that filed certain forms with a Registration Agency in its Jurisdiction, the Registration Agency issued or approved the entity's charter, certificate, or license, and the entity's 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 entity (owners, partners, managing members, directors or officers) is identified and validated by the CA; • the identified Principal Individual (owners, partners, managing members, directors or officers) attests to the representations made in the Subscriber agreement; • the CA verifies the entity's use of any assumed name, used to represent the entity pursuant to the requirements of Section 3.2.5;	3.2.2.3

#	Criterion	VMCRRef
2.3 *(cont'd)*	• the entity and the identified Principal Individual (owners, partners, managing members, directors or officers) associated with the entity are 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 and the identified Principal Individual (owners, partners, managing members, directors or officers) associated with the entity are not listed on any published government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.	
2.4	The CA maintains controls to provide reasonable assurance that it issues VMC to Non-Commercial Entities, defined within the VMCR as applicants that meet the following requirements: • 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; • the Applicant is not 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 Applicant is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.	3.2.2.4

Certificate content and profile

#	Criterion	VMCRRef
2.5	The CA maintains controls to provide reasonable assurance that VMC issued include the minimum requirements for the content of VMC, including: • Certificate Policy Identification requirements • Subscriber Public Key • Certificate Serial Number • Additional Technical Requirements for EV Certificates as established in the VMCR relating to: • VMC Subscriber Certificates • VMC Subordinate CA Certificates	6.1.5, 7.1

2.6	The CA maintains controls to provide reasonable assurance that except as otherwise expressly specified by VMCR Section 7, VMCs must comply with all requirements of the EV Guidelines Sections 9.2 (Subject Identity) and 9.3 (Certificate Policy Identification), Version 1.7.5.	7.1
2.7	The CA maintains controls to provide reasonable assurance that the CA generates non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.	7.1
2.8	The CA maintains controls to provide reasonable assurance that the version of certificates issued are of type x.509 v3.	7.1.1
2.9	The CA maintains controls to provide reasonable assurance that the subject information, extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Root CA certificates generated conform to the VMCR.	7.1.2.1, 6.1.5.1, 7.1.6.1, 7.1.4.3
2.10	The CA maintains controls to provide reasonable assurance that the subject information, extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Subordinate CA certificates conform to the VMCR.	7.1.2.2, 6.1.5.2, 7.1.4.3
2.11	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 VMCR.	7.1.2.3, 6.1.5.3
2.12	The CA maintains controls to provide reasonable assurance that with exception to the requirements stipulated in the VMCR Sections 7.1.2.1, 7.1.2.2, and 7.1.2.3, all other fields and extensions of certificates generated are set in accordance with RFC 5280.	7.1.2.4
2.13	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 VMCR.	6.3.2
2.14	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 intended use, unless: 1. Such values fall within an OID arc for which the Applicant demonstrates ownership; or 2. The Applicant can otherwise demonstrate the right to assert the data in public context	7.1.2.4

#	Criterion	VMCRRef
2.15	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
2.16	The CA maintains controls to provide reasonable assurance that it does not issue any Subscriber or Subordinate CA certificates using the SHA-1 hash algorithm and does not continue to use existing SHA-1 Root Certificates for VMCs.	7.1.3
2.17	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.	7.1.4.3
2.18	The CA maintains controls to provide reasonable assurance that CAs must not include the nameConstraints extension in Certificates.	7.1.5

Certificate request requirements

#	Criterion	VMCRRef
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; and 2. An executed Subscriber or Terms of Use Agreement.	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); • certified as to being correct by the applicant; and • contains the information specified in Section 4.2.1 of the VMCR.	4.1.2, 4.2.1

Subordinate CA private keys

#	Criterion	VMCRRef
3.3	The CA maintains controls to provide reasonable assurance that it does not archive the Subordinate CA Private Keys. Additionally: • If the CA or any of its designated RAs generated the Private Key on behalf of the Subordinate CA, then the CA shall encrypt the Private Key for transport to the Subscriber or Subordinate CA. • If the CA becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the 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 Subordinate CA Private Key if it receives authorisation from the Subordinate CA.	6.2.5, 6.2.6

Subscriber agreements and terms of use

#	Criterion	VMCRRef
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 VMCR Section 9.6.4 that is signed by an authorized Contract Signer and contains provisions imposing obligations and warranties on the Application relating to: • the accuracy of information • acceptance of certificate • use of certificate • reporting and revocation • responsiveness • acknowledgement and acceptance.	3.2.11, 9.6.4

Information verification requirements

Verification of applicant's legal existence and identity

#	Criterion	VMCRRef
4.1	The CA maintains controls to provide reasonable assurance that the following information provided by the Applicant is verified by performing the steps established by the VMCR: For Private Organization Subjects: • legal existence and identity • legal existence and identity – assumed name • organization name • registration number • registered agent • relationship to the parent, subsidiary, or affiliate (if applicable) For Government Entities: • legal existence • entity name • registration number For Business Entities: • legal existence • organization name • registration number • principal individual • relationship to the parent, subsidiary, or affiliate (if applicable) For Non-Commercial Entities: • International Organization Entities — legal entities — entity name — registration number For entities the Subject organization information is verified directly by performing the steps established by the VMCR: • the entities operational existence • the entity is a registered holder, or has control, of the Domain Name(s) included in the VMC • a reliable means of communication with the entity to be named as the Subject in the Certificate	3.2.2.1, 3.2.2.2, 3.2.2.3, 3.2.2.4, 3.2.3, 3.2.4, 3.2.5, 3.2.6

#	Criterion	VMCRRef
4.1 *(cont'd)*	• Verify the Applicant's authorization for the Verified Mark Certificate, including; — Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester, — Verify that a Contract Signer signed the Subscriber Agreement or that a duly authorized individual acknowledged and agreed to the Terms of Use; and — Verify that a Certificate Approver has signed or otherwise approved the Verified Mark Certificate Request.	

Verification of applicant

#	Criterion	VMCRRef
4.2	The CA maintains controls to provide reasonable assurance that it verifies the physical address provided by Applicant is an address where Applicant or a Parent /Subsidiary company conducts business operations (e.g., not a mail drop or P.O. box, or 'care of' C/O address, such as an address of an agent of the Organization), and is the address of Applicant's Place of Business using a method of verification established by the VMCR.	3.2.7.1
4.3	The CA maintains controls to provide reasonable assurance that it verifies a telephone number, fax number, email address, or postal delivery address as a Verified Method of Communication with the Applicant by performing the steps set out in the VMCR.	3.2.8.1, 3.2.8.2
4.4	The CA maintains controls to provide reasonable assurance that it verifies Applicant's, or Affiliate/Parent/Subsidiary Company's operational existence by: • verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has been in existence for at least three years, as indicated by the records of an Incorporating Agency or Registration Agency; • verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company is listed in either a current QIIS or QTIS;	3.2.9.1, 3.2.9.2

#	Criterion	VMCRRef
4.4 *(cont'd)*	• verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has an active current Demand Deposit Account with a Regulated Financial Institution by receiving authenticated documentation of the Applicant's, Affiliate's, Parent Company's, or Subsidiary Company's Demand Deposit Account directly from a Regulated Financial Institution; or • relying on a Verified Legal Opinion or a Verified Accountant Letter to the effect that the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution.	

Verification of Contract Signer and Approver

#	Criterion	VMCRRef
4.5	The CA maintains controls to provide reasonable assurance that it verifies, using a method of verification established by the VMCR: • 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 VMC Request to: — submit, and if applicable authorize a Certificate Requester to submit, the VMC Request on behalf of the Applicant; — provide, and if applicable authorize a Certificate Requester to provide, the information requested from the Applicant by the CA for issuance of the VMC; and — approve VMC Requests submitted by a Certificate Requester.	3.2.10.1, 3.2.10.2, 3.2.10.3, 3.2.10.4
4.6	The CA maintains controls to provide reasonable assurance that it conducts face-to-face validation of the Contract Signer or Certificate Approver for the Applicant following the validation steps described in Appendix G of the VMCR.	3.2.10.1

#	Criterion	VMCRRef
4.7	The CA maintains controls to provide reasonable assurance, using a method of verification established in the VMCR that: • subscriber Agreements are signed by an authorized Contract signer; • the VMC Request is signed by the Certificate Requester submitting the document; • if the, Verified Mark Certificate Request is signed and submitted by a Certificate Requester who does not also function as a Certificate Approver, approval and adoption of the Verified Mark Certificate Request by a Certificate Approver in accordance with the requirements of VMCR, Section 3.2.12 can substitute for authentication of the signature of the Certificate Requester on such Verified Mark Certificate Request • signatures have been authenticated, in accordance with VMCR, Section 3.2.11.2.	3.2.11

Verification of VMC certificate requests

#	Criterion	VMCRRef
4.8	The CA maintains controls to provide reasonable assurance that in cases where an VMC Request is submitted by a Certificate Requester, before it issues the requested VMC, it verifies that an authorized Certificate Approver reviewed and approved the VMC Request.	3.2.12
4.9	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 VMCR. 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 status of the author, — the basis of the opinion, and — authenticity.	3.2.13

#	Criterion	VMCRRef
4.9 *(cont'd)*	• 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 VMCR, Section 3.2.13.5. — the CA follows a documented process to check the accuracy of the database and ensure its data is acceptable, including reviewing the database provider's terms of use — othe CA does not use any data in a QIIS that the CA knows is (i) self-reported and (ii) not verified by the QIIS as accurate • with respect to Qualified Government Information Sources (QGIS) • the database used is a QGIS as defined by the VMCR, Section 3.2.13.6. • 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 VMCR, Section 3.2.13.7.	

Verification of domain control

#	Criterion	VMCRRef
4.10	The CA maintains controls to provide reasonable assurance that prior to issuing a Certificate the CA obtains confirmation in accordance with one of the allowed methods in the VMCR Section 3.2.14 related to the Fully-Qualified Domain Name(s) (including wildcard domains). The CA maintains records of which validation method, including the relevant VMCR version number, used to validate every domain.	3.2.14

Certificate authority authorization (CAA) checking

#	Criterion	VMCRRef
4.11	The CA maintains controls to provide reasonable assurance that as part of the issuance process, it checks for CAA records, and, if present, processes these records and issues certificates in accordance with the requirements set forth in Section 3.2.15 of the VMCR.	3.2.15
4.12	The CA maintains controls to provide reasonable assurance that it documents potential certificate issuances that were prevented by a CAA record.	3.2.15

Registered mark verification

#	Criterion	VMCRRef
4.13	The CA maintains controls to provide reasonable assurance the CA confirms that the Mark Representation submitted by the Subject organization matches the Registered Mark in accordance with Section 3.2.16.1 of the VMCR.	3.2.16.1, Appendix E
4.14	The CA maintains controls to provide reasonable assurance the CA confirms that the Registered Mark identified in the official database of the applicable Trademark Office or the WIPO Global Brand Database is the same Subject organization verified by the Verified Mark vetting process in accordance with Section 3.2.16.2 of the VMCR.	3.2.16.2

#	Criterion	VMCRRef
4.15	The CA maintains controls to provide reasonable assurance the CA confirms that the Mark Representations in Verified Mark Certificates for Combined Marks and Design Marks shall only be in colours as permitted for the Registered Mark by the applicable Trademark Office in accordance with Section 3.2.16.1.3 of the VMCR.	3.2.16.1.3

Verification of other

#	Criterion	VMCRRef
4.16	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 to identify subsequent suspicious certificate requests.	3.2.17
4.17	The CA maintains controls to provide reasonable assurance that no Verified Mark 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.	3.2.17
4.18	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 to identify subsequent suspicious certificate requests.	4.1.1

Validation for existing subscribers

4.19	The CA maintains controls to provide reasonable assurance that validation data is only reused when the data was gathered less than 398 days ago. Additional face-to-face validation is not required if the stipulations of VMCR, Section 4.2.1, are met.	4.2.1

Certificate issuance by a Root CA

#	Criterion	VMCRRef
4.20	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
4.21	The CA maintains controls to provide reasonable assurance that Root CA Private Keys are not used to sign Certificates except in the following cases: 1. Self-signed Certificates to represent the Root CA itself; 2. Certificates for Subordinate CAs and Cross Certificates which contain id-kp-BrandIndicatorforMessageIdentificat ion (OID: 1.3.6.1.5.5.7.3.31) as the sole KeyPurposeId in the extendedKeyUsage extension; 3. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and 4. Certificates for OCSP Response verification.	6.1.7
4.22	The CA maintains controls to provide reasonable assurance that Subordinate or Cross Certificates are not used to sign Certificates unless the following OIDs contain the sole KeyPurposeId in the extendedKeyUsage extension: 1. id-kp-BrandIndicatorforMessageIdentification (OID: 1.3.6.1.5.5.7.3.31); or 2. b. id-kp-OCSPSigning (OID: 1.3.6.1.5.5.7.3.9)	6.1.7

Other matters

#	Criterion	VMCRRef
4.23	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 in Section 5.3.3. 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.	3.2.18
4.24	The CA maintains controls to provide reasonable assurance that before a certificate issued a pre-certificate is logged in a Certificate Transparency log in accordance with VMCR, Section 4.3.1 and Appendix F.	4.3.1

Certificate revocation and status checking

#	Criterion	VMCRRef
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

#	Criterion	VMCRRef
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 and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report: • decides whether revocation or other appropriate action is warranted; • if revocation is deemed the appropriate action, the elapsed time from receipt of the Certificate Problem Report or revocation request and revocation status information does not exceed the timelines in VMCR 4.9.1.1; 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 validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon. And, Subscriber Certificates are revoked within 5 days if any of the following events occurs 1. The Certificate no longer complies with the requirements of VMCR Sections 6.1.5 and 6.1.6; 2. The CA obtains evidence that the Certificate was misused; 3. 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;	4.9.1.1

#	Criterion	VMCRRef
5.3 *(cont'd)*	4. 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); 5. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name; 6. The CA is made aware of a material change in the information contained in the Certificate; 7. 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; 8. The CA determines that any of the information appearing in the Certificate is inaccurate; 9. 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; 10. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or	
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 VMCR 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 VMCRor the applicable Certificate Policy or Certification Practice Statement;	4.9.1.2

#	Criterion	VMCRRef
5.4 *(cont'd)*	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; or 9. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement;	
5.5	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: — 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 — 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 Subscriber Certificates: • for the status of subordinate CA Certificates — 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 — 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 VMCR.	4.9.7, 4.9.10, 4.10.2
5.6	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

#	Criterion	VMCRRef
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 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
5.9	The CA maintains controls to provide reasonable assurance that OCSP responses by CA's which have not been technically constrained in accordance with VMCR 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

#	Criterion	VMCRRef
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 disclosed in CA's Certificate Policy and/or Certification Practice Statement, common threats to the information verification process, and the VMCR; • the CA maintains records of such training;	5.3.3, 5.3.4

#	Criterion	VMCRRef
6.2 *(cont'd)*	• the CA documents each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task; and • the CA requires all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the Baseline Requirements.	
6.3	The CA maintains controls to provide reasonable assurance that Delegated Third Parties meet the qualification requirements of Section 5.3.3 of the VMCR.	5.3.7
6.4	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

Data records

#	Criterion	VMCRRef
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

#	Criterion	VMCRRef
7.2	The CA maintains controls to provide reasonable assurance that the following events are recorded: • CA key lifecycle management events, including: — Key generation, backup, storage, recovery, archival, and destruction; — Certificate requests, renewal, and re-key requests, and revocation; — Approval and rejection of certificate requests; — Cryptographic device lifecycle management events; — Generation of Certificate Revocation Lists and OCSP entries; — Introduction of new Certificate Profiles and retirement of existing Certificate Profiles. • Subscriber Certificate lifecycle management events, including: — Certificate requests, renewal, and re-key requests, and revocation; — All verification activities stipulated in these Requirements and the CA's Certification Practice Statement; — Approval and rejection of certificate requests; — Issuance of Certificates; and — Generation of Certificate Revocation Lists and OCSP entries. • security events, including: — Successful and unsuccessful PKI system access attempts; — PKI and security system actions performed; — Security profile changes; — Installation, update and removal of software on a Certificate System; — System crashes, hardware failures, and other anomalies; — Firewall and router activities; and — Entries to and exits from the 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	5.4.1
7.3	The CA maintains controls to provide reasonable assurance that audit logs are retained for two years in accordance with VMCR, Section 5.4.3.	5.4.3

#	Criterion	VMCRRef
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 two years after any Certificate based on that documentation ceases to be valid.	5.5.2

Audit and legal

#	Criterion	VMCRRef
8.1	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 the greater of one certificate and at least three percent (3%) of the VMC issued during the period commencing immediately after the previous self-assessment samples were taken.	8.7
8.2	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 VMCs.	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	VMCRRef
1.1	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, (WTCA v2.2.1 Sec 3.1)
1.2	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 (WTCA v2.2.1 Sec 3.1)

#	Criterion	VMCRRef
1.3	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: • 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.	5.0 (WTCA v2.2.1 Sec 3.1)
1.4	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;	5.7.1 (WTCA v2.2.1 Sec 3.8)

#	Criterion	VMCRRef
1.4 *(cont'd)*	• 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.	
1.5	The CA maintains controls to provide reasonable assurance that its Certificate Management Process includes: • physical security and environmental controls; • system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention • network security and firewall management, including port restrictions and IP address filtering; • user management, separate trusted-role assignments, education, awareness, and training; and • logical access controls, activity logging, and inactivity time-outs to provide individual accountability.	5.0 (WTCA v2.2.1 Sec 3.4)
1.6	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
1.7	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 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.

General protections for the network and supporting systems

#	Criterion	VMCRRef
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 are applied to all systems co-located within the same network as a Certificate System.	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

#	Criterion	VMCRRef
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
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 Multi-Factor Authentication.	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

#	Criterion	VMCRRef
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, and group accounts or shared role credentials are not used.	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: — Passwords have at least twelve (12) characters • For authentications which cross a zone boundary into a Secure Zone or High Security Zone: — Require Multi-Factor Authentication	2.g

#	Criterion	VMCRRef
2.7 *(cont'd)*	• For accounts accessible from outside a Secure Zone or High Security Zone: — Passwords to have at least eight (8) characters, not be one of the user's previous four (4) passwords; and implement account lockout for failed access attempts in accordance with requirement 2.k (Criterion 2.11); • Effective 1 April 2020, routine password changes are completed no more frequently than once every two years.	
2.8	The CA maintains controls to provide reasonable assurance that it has a policy for Trusted Roles to log out of or lock workstations when no longer in use.	2.h
2.9	The CA maintains controls to provide reasonable assurance that it has a procedure to configure workstations with inactivity time-outs that log the user off or lock the workstation after a set time of inactivity without input from the user, and that workstations are configured in accordance with the policy.	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 Authentication OR multi-party authentication for administrator access to Issuing Systems and Certificate Management Systems.	2.m

#	Criterion	VMCRRef
2.14	The CA maintains controls to provide reasonable assurance that it enforces Multi-Factor Authentication for all Trusted Role accounts for both itself and Delegated Third Parties on Certificate Systems (including those approving the issuance of a Certificate) that are accessible from outside a Secure Zone or High Security Zone.	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: — Located within the CA's network; — Secured in accordance with the Network and Certificate System Security Requirements; and — Mediates the remote connection to the Issuing System.	2.o

Logging, monitoring, and alerting

#	Criterion	VMCRRef
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

#	Criterion	VMCRRef
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 it monitors the integrity of the logging processes for application and system logs through continuous automated monitoring and alerting or through a human review to ensure that logging and log-integrity functions are effective. Alternatively, if a human review is utilized and the system is online, the process must be performed at least once every 31 days	3.e
3.6	The CA maintains controls to provide reasonable assurance that it monitors the archival and retention of logs to ensure that logs are retained for the appropriate amount of time in accordance with the disclosed business practices and applicable legislation	3.f
3.7	The CA maintains controls to provide reasonable assurance that If continuous automated monitoring and alerting is utilised to satisfy Network Security Requirements 1.h. or 3.e. that it responds to the alert and initiates a plan of action within at most twenty-four (24) hours.	3.g

Vulnerability detection and patch management

#	Criterion	VMCRRef
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

#	Criterion	VMCRRef
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: — 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 — 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: — The CA disagrees with the NVD rating; — The identification is a false positive; — The exploit of the vulnerability is prevented by compensating controls or an absence of threats; or — Other similar reasons.	4.f

Appendix A: External Documents

These Criteria are based on the following documents:

Document Name	Publisher	Version	Issuance Date
Minimum Security Requirements for Issuance of Verified Mark Certificates	Authindicators Working Group	1.0	9 July 2021
Network and Certificate System Security Requirements	CA Browser Forum	1.7	5 April 2021
Guidelines for the Issuance and Management of Extended Validation	CA Browser Forum	1.7.5	5 April 2021

Copies of these documents are available on the respective websites at https://cabforum.org/documents and https://bimigroup.org/supporting-documents/.

The VMCR may also be updated from time to time and the practitioner is not required to consider these updated versions until reflected in the subsequently updated WebTrust Criteria. The practitioner is directed to review the current version of the VMCR history, revisions, and relevant dates to understand the applicability of certain Guidelines and Requirements.

Appendix B: Sections of VMCR Requirements not subject to assurance

Sections of the VMCR which contain no content or the phrase “No Stipulation” were not considered. Additionally, the following items are not subject to assurance:

Ref	Topic	Reasons for exclusion
1.1	Overview	Information only
1.3 (except 1.3.2)	PKI Participants	Information only
1.4	Certificate Usage	Information only
1.5 (except 1.5.2)	Policy Administration	Information only
1.6	Definitions and Acronyms	The practitioner is directed to consider these definitions when interpreting the VMCR and these criteria.
4.9.2	Who Can Request Revocation	Information only
8.2	Identity/Qualifications of Assessor	Information only
8.6	Communication of Results	Information only
9.6	CA Representations and Warranties	Legal item
9.16.3	Severability	Legal item