ABC Certification Authority, Inc.

Report on Description of its Certification Authority System and Design, Implementation and Operating Effectiveness of PKI Controls for the period January 1, 20XX, to December 31, 20XX

Insert report restriction

Table of Contents

Independent Service Auditor's Report

Independent Service Auditor's Report[1]

To the Management of ABC Certification Authority, Inc.

Scope

We have examined ABC Certification Authority, Inc.'s ("ABC-CA") accompanying description in section 3 titled " ABC Certification Authority, Inc.'s Description of its Certification Authority System" throughout the period January 1, 20XX, to December 31, 20XX, (description)2 based on the CA Description Requirements for a description of a certification authority system set out in WebTrust for Certification Authorities 2019 Description Requirements for a Description of a Certification Authorities System (CPA Canada, CA Description Requirements), (description requirements) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that ABC-CA's of meeting the criteria set forth in the WebTrust Principles and Criteria for Certification Authorities Vs2.x3 and the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x (applicable WebTrust criteria).

The information included in section 5, "Other Information Provided by ABC-CA That Is Not Covered by the Service Auditor's Report," is presented by ABC-CA management to provide additional information and is not a part of the description. Information about ABC-CA's [*describe the nature of the information, for example, responses to identified exceptions*] has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve the applicable WebTrust criteria.

Certification Authority's Responsibilities

ABC-CA is responsible for designing, implementing, and operating effective controls within the system to achieve the applicable WebTrust criteria. In section 2, ABC-CA has provided its assertion titled "Assertion of ABC Certification Authority Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. ABC-CA is also responsible for preparing the description and assertion, including the

[1] The report may also be titled "Report of Independent Service Auditors."

[2] The title of the description of the service organization's system in the service auditor's report should be the same as the title used by service organization management in its description of the service organization's system.

[3] Include applicable version number and hyperlink to the criteria document

completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable achieve the applicable WebTrust criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of ABC-CA ’s applicable WebTrust criteria.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description requirements and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that ABC-CA’s applicable WebTrust criteria were achieved. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of ABC-CA’s system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and ABC-CA’s applicable WebTrust criteria
- Assessing the risks that the description is not presented in accordance with the description requirements and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description requirements
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the applicable WebTrust criteria were achieved
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that ABC-CA’s applicable WebTrust criteria were achieved
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Insert report restriction

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the registration authority's service commitments and system requirements are achieved based on the applicable WebTrust criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in section 4, " WebTrust Principles and Criteria for Certification Authorities, Related Controls, and Tests of Controls."

Opinion

In our opinion, in all material respects,

a. the description presents ABC-CA's certification authority system that was designed and implemented throughout the period January 1, 20XX, to December 31, 20XX, in accordance with the description requirements.

b. the controls stated in the description were suitably designed throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that ABC-CA's the applicable WebTrust criteria would be achieved, if its controls operated effectively throughout that period.

c. the controls stated in the description operated effectively throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that ABC-CA's applicable WebTrust criteria were achieved.

Restricted Use

This report, including the des*cr*iption of tests of controls and results thereof in section 4, is intended solely for the information and use of ABC-CA, subscribers of ABC-CA's certification authority system during some or all of the period January 1, 20XX, to December 31, 20XX, business partners that include internet browsers whose Trust Programs are members of, and practitioners providing services to such subscribers and, prospective subscribers and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the certification authority
- How the certification authority's system interacts with subscriber, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Subscriber responsibilities and how they may affect the user entity's ability to effectively use the certification authority's services

Insert report restriction

- The applicable criteria for certification authorities
- The risks that may threaten the achievement of the certification authority's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

[Service auditor's signature]

[Service auditor's city and state]

[Date of the service auditor's report]

Section 2 - Illustrative Assertion by Certification Authority Management

[ABC Certification Authority, Inc. Letterhead]

Assertion of ABC Certification Authority, Inc. Management

We have prepared the accompanying description of ABC Certification Authority, Inc.'s ("ABC-CA") titled "ABC Certification Authority, Inc.'s Description of its Certification Authority System" throughout the period January 1, 20XX, to December 31, 20XX, (description)[4] based on the criteria for a description of a certification authority system set out in WebTrust for Certification Authorities *2019 Description Requirements for a Description of a Certification Authorities System* (CPA Canada, *CA Description Criteria*), (description requirements) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that ABC-CA's of meeting the criteria set forth in the *WebTrust Principles and Criteria for Certification Authorities Vs2.x*[5] and *WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x* (applicable WebTrust criteria).

The management of ABC-CA is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website [or other repository location][6], CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

ABC-CA management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in ABC-CA management's opinion, in providing its CA services, throughout the period January 1, 20XX, to December 31, 20XX, ABC-CA confirms, to the best of its knowledge and belief, that:

a) the description presents ABC-CA's certification authority system that was designed and implemented throughout the period January 1, 20XX, to December 31, 20XX, in accordance with the description requirements.

[4] The title of the description of the service organization's system in the service auditor's report should be the same as the title used by service organization management in its description of the service organization's system.

[5] Include applicable version number and hyperlink to the criteria document

[6] Link to business practices repository location and describe location if not website (i.e. intranet)

Insert report restriction

b) the controls stated in the description were suitably designed throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that ABC-CA's would achieve the applicable WebTrust criteria, if its controls operated effectively throughout that period.

c) the controls stated in the description operated effectively throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that ABC-CA met the applicable WebTrust criteria.

Section 3

ABC Certification Authority, Inc.'s Description of its Certification Authority System

Scope and Boundaries of the System

ABC-CA is a Certification Authority (CA) based in the United States that provides global digital certificate services with the support of its corporate subsidiaries, (collectively referred to as "ABC-CA"), based in the United States, Japan and Canada. ABC-CA offers trusted identity and secure transaction technologies that provide digital identity solutions for businesses of all sizes – protecting employees, customers, intellectual property and overall brand. As a commercial certificate authority with over 200 million TLS/SSL certificates issued worldwide, ABC-CA has over 20 years of experience and performance to meet the growing need to secure transactions and create online trust.

ABC-CA's team addresses the digital security challenges for individuals, e-merchants, small to medium businesses, and large enterprises. ABC-CA's software and services do this by authenticating individuals, devices and business websites and securing information through strong public key encryption.

This report addresses the following criteria for the period Month XX, 20XX to Month XX, 20XX:

- WebTrust Principles and Criteria for Certification Authorities, Version 2.X
- WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, Version 2.X

Repository

ABC-CA maintains a Repository which comprises its root certificates, its current Certificate Policy ("CP"), Certification Practice Statement ("CPS"), Subscriber Agreements, Relying Party Agreements, and the most recent revocation information for certificates it has issued.

Additionally, ABC-CA publishes all non-constrained Subordinate CA certificates and its commitment to adherence to the latest version of the policy documents published on its Repository. The Repository can be accessed at http://abc-ca.repository.xx.

Services Provided

ABC-CA's Digital Certificate Solutions offer a wide range of hosted products with the flexibility and technical capability to meet customized Customer PKI needs. The following are offered through this product line:

Insert report restriction

- TLS (Transport Layer Security)/SSL (Secure Socket Layer) encryption using SHA-256 and 2048-bit RSA keys as standard.
- Extended Validation (EV) SSL
    - Multi-Domain EV SSL
    - Wildcard SSL
- ABC Advanced
    - General Purpose SSL
    - Secure E-mail – S/MIME
    - Client Authentication
    - Code Signing
    - EV Code Signing
    - Personal Authentication

ABC-CA provides the following CA services:

CA Business Practices Disclosure

- Certificate Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- System Development, Maintenance, and Change Management
- Disaster Recovery, Backups, and Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival
- CA Key Destruction

Insert report restriction

- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Transportation
- CA Key Migration

Subscriber Key Lifecycle Management Controls

- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subscriber Key Lifecycle Management

- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Key Storage and Recovery Services
- Integrated Circuit Card (ICC) Lifecycle Management
- Requirements for Subscriber Key Management

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

ABC-CA does not escrow its CA keys and does not provide certificate suspension services. Accordingly, this system description does not extend to controls that would address those criteria.[7]

Detailed Audit of Certificate System - Coverage

The CAs in scope are set out in Attachment 1 at the end of the Description along with relevant CA Identifying information. Changes to the list of in scope CAs that were made during the examination period (set out information as to additions, retirements etc.) are also enumerated in this attachment.

The following CAs that form part of the ABC-CA hierarchy are not in scope for this examination as they are operated by a third party and audited and reported under a separate cover:

(list CAS that are not in scope and reason thereof- can be done in tabular format).

[7] All services not provided should be listed here and removed from the list above.

ABC-CA operates under a publicly available combined CP/CPS that was developed under RFC 3647. It is available at www. ABC.com/pki/cps. The version(s) applicable to the examination were Version 7.0 (to June 30) and Version 7.1 (from July 1 to end of period) (also can be displayed in tabular format). These should be referred to as they form an integral part of this system description.

Scope of the Description

The scope of this Description has been prepared to provide information on specified processes and controls of ABC-CA, based on the CPA Canada Disclosure Requirements for PKI. The Scope of this Description includes the production systems of ABC-CA's Digital Certificate Solutions that are hosted within the following San Francisco, Toronto and Tokyo locations. All CA and RA services are provided under a dual primary model from the San Francisco and Toronto locations. The Tokyo location provides RA services, as well as hosting cold storage for key materials and additional online services providing certificate validation status.

System Incidents

In order to ensure that incidents are being recorded as per the procedure and that investigation and resolution are completed in a reasonable time, reviews of incident reports are carried out by the Compliancy Team on a quarterly basis. The review takes a sample of reports and analyzes them for completeness. Any findings are raised to the incident handler, asset owner and/or senior management.

In addition to system incidents, ABC-CA monitors and tracks compliance related events. Compliance incidents can impact any of the following requirements:

- Internally defined policies and procedures
- CP/CPS procedures and legal requirements
- CA Browser Forum Baseline requirements
- Third-party trusted root program requirements

Compliance incidents follow the same processes as above, with the exception of evaluation for external reporting. Compliance incidents for an external facing requirement, are reported to the proper authority based on that authority's reporting requirements. The following compliance events occurred during the period.

Mozilla Bug # Link	Description	Date Reported	Date Resolved

Components of the CA System Used to Provide the Services

Infrastructure

Systems providing online certificate issuance (e.g. Issuer CAs) are located in corporate data centers that are located in San Francisco and Toronto. The San Francisco data center is operated by QRS Data Storage, Inc. and the Toronto location is operated by XYZ Data Centers, Inc. ABC-CA has implemented controls in addition to those provided by the data center to protect online equipment (including certificate status servers and CMS equipment) from unauthorized access and implements physical controls to reduce the risk of equipment tampering. These controls include physical barriers, such as a dedicated caged environment, with two person and two factor access controls. ABC-CA has also implemented video surveillance monitoring in addition to the services provided by the third-party data center. The data centers provide various layers of external security barriers, security personnel on duty full time (24 hours per day, 365 days per year), and environmental controls.

Software

ABC-CA's Certificate Manager

ABC-CA's Certificate Manager (SCM) is an internally developed solution that offers customers:

- Centralized administration of digital certificates.
- Secure, multi-tiered web interface for administering digital certificates.
- Certificate discovery that scans the network to pinpoint and record certificate deployments.
- Securely hosted across multiple co location data centers thus providing high availability & disaster recovery features.
- Configurable email alerts for pending administrative tasks.
- Life-cycle administration for ABC-CA's portfolio of certificates.
- Customer key escrow that enables a protected recovery of user encrypted data.

SCM is hosted in the third-party data centers described in the prior section.

ABC-CA uses a combination of industry standard and proprietary software (i.e., applications) to support the SCM systems. Software includes the following:

- Linux based systems

- Name of network operating system
- Windows Domain servers
- Databases: Oracle and LIST OTHER DATABASES
- Applications for the lifecycle issuance and management of certificates:
    - Name of system - order management of certificates
    - Name of system - validation of certificates
    - ABC-CA Certificate Manager - The certificate life cycle management
    - Others – list
- PKI management offerings from leading industry providers (for example nCipher, Genalto etc)

Access to and use of this software and utilities are restricted to appropriate ABC-CA Personnel.

People

Organizational Structure – General and Trusted Roles

ABC-CA's organizational structure provides a framework for planning, directing, & controlling business operations. ABC-CA's personnel and business functions are segregated into specific departments according to product & operational responsibilities, with defined job responsibilities and lines of authority for reporting & communication.

ABC-CA's business operations are directed by the executive management team (Chief Executive Officer (CEO), Chief Financial Officer (CFO), Chief Information Officer (CIO), Chief Compliance Officer (CCO) & Chief Technology Officer (CTO)). This cross functional management team provides overall executive guidance and support for the planning and execution of the day to day operations of ABC-CA, supporting the Compliancy and Infrastructure teams that develop, monitor and manage ABC-CA's overall control objectives and control activities, and the communicating and monitoring ABC-CA's internal control policies and procedures.

The Compliancy team (inclusive of the 'Policy Authority') is responsible for the effective development and implementation of ABC-CA's Information Security Policy & supporting documentation, including the CP/CPS. The team communicates the Information Security Policy to ABC-CA's employee's, and monitors the effectiveness of ABC-CA's controls as well as employee and system compliance to documented policies.

The Infrastructure team is responsible for providing core IT support services throughout the ABC-CA group of companies. The protection of IT systems and the information they store, technical evaluation of systems, access administration, access control, desktop support and hosting support is provided by the Infrastructure team.

Trusted Roles

Personnel acting in trusted roles include CA and RA system administration personnel and personnel involved with identity vetting and the issuance and revocation of Certificates. The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI or TSA operations.

All Personnel

Back office processing for ABC-CA's Digital Certificate Solutions and SCM systems, business development and management functions operate from ABC-CA's office locations. All personnel are recruited as per ABC-CA's HR procedures.

Procedures

ABC-CA has documented policies, procedures, and supporting documents that support the operations and controls over its systems in support of the Digital Certificate Solutions and SCM systems. ABC-CA further publishes these policies and procedures through the use of an internal repository, making them available to ABC-CA employees. The public CP/CPS should also be referred to.
Procedures, as discussed in this report, cover the following areas:

- Policy development and management
- Physical and environmental security
- Logical security
- Network security
- Change management

Data

Customer data supplied to ABC-CA in support of their account or certificate order(s) is treated as confidential with access to data throughout its lifecycle appropriately restricted. Data received is stored electronically by the applicable system/application in the corresponding database. ABC-CA applies a default deny policy to all information it holds with access limited to a 'need to know' basis following controlled processes for granting, removing, and renewing access. FIPS approved encryption algorithms is utilized to protect data in transit and when stored on backup media. Any hardcopy data is stored in secure cabinets and routinely destroyed when no longer required.

Description of the Controls Relevant to WebTrust Principles

Insert report restriction

Principle 1 – CA Business Practices Disclosure

Certification Practice Statement (CPS) and Certificate Policy (CP)
[Insert client specific information]

Principle 2 – CA Business Practices Management

CPS Management, CP Management, and CP and CPS Consistency
[Insert client specific information]

Principle 3 - CA Environmental Controls

Security Management

ABC-CA has developed and implemented a formal security architecture based on industry standard security practices. ABC-CA's security architecture is supported by formal policies & procedures and backed by senior management's commitment to information security. Policies, procedures and supporting documentation are updated regularly by their document owners based on business and technological challenges posed with approval from members of the ABC-CA management team.

ABC-CA's information security policies apply to all ABC-CA personnel (whether full time or part time, permanent, and probationary or contract) who use ABC-CA information or business systems, irrespective of geographic location or department. Third parties accessing ABC-CA information or systems are required to adhere to the general principles of this policy, and other security responsibilities and obligations with which they must comply. ABC-CA's Information Security Policy covers the following control objectives:

- Information Security
- Physical & Environmental Security
- Logical Access
- Change Management
- Incident Management
- Application/System Development & Maintenance
- Human Resource Security
- Malicious Code Protection & Vulnerability Management
- Logging & System Monitoring
- ETC

Risk Assessment

ABC-CA has adopted a risk assessment process to pro-actively identify, monitor and manage business and operational risks. The risk assessment process focuses on identifying, assessing and mitigating identified risks to ABC-CA's assets. The Compliancy Team oversees and monitors ABC-CA's risk assessment activities, including management's actions to address any identified significant risks. The risk management process consists of the following activities:

- Risk Assessment
- Asset Register, Business Impact Assessment
- Threat & Vulnerability Assessment
- Likelihood Assessment
- Risk Measure
- Risk Treatment
- Risk Measure Review
- Risk Treatment Decision
- Control Selection & Implementation and Residual Risk

Vendor (Third-Party) On-boarding & Risk Management Program

ABC-CA maintains a third-party vetting program for all new and existing vendors. Vendors are required to sign contractual agreements which outline the vendor's security and availability commitments and responsibilities.

At point of vendor creation (after vendor acceptance), each vendor is categorized by vendor risk profile and classified into Critical, High, Medium or Low risk categories. All third parties are monitored on an ongoing basis as part of the quarterly internal audit process (compliancy checks once ABC-CA has business requirements to maintain its vendors). The level of Supplier service monitoring is based on the suppliers' classification. All Critical & High classified suppliers are monitored internally through direct and/or indirect means. Vendor Service Level Agreements (SLA)s, along with service performance levels, are reviewed by the Compliance Team on a regular basis through service reports and records to ensure SLAs are defined and that they are being adhered to. Any findings from the review are highlighted back to management/Asset Owner through a formal reporting process.

Vulnerability Scanning
[Insert client specific information]

Penetration Testing
[Insert client specific information]

<u>Asset Classification and Management</u>
[Insert client specific information]

<u>Personnel Security</u>

Insert report restriction

Formal hiring procedures are employed to ensure all new employees are qualified for their assigned duties. The recruiting process is the joint responsibility of the Human Resource (HR) department and the relevant business department managers. Hiring decisions are based on various factors including educational background, prior experience, and past accomplishments.

All candidates must undergo background checks in line with local employment law and practices. In addition to the above, all persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness and integrity.

All employment offers are conditional on the candidate agreeing to, and signing the terms and conditions detailed in their employment contract, including confidentiality and non-disclosure agreements, as well as the employee handbook and ABC-CA's internal policies. It is required that all personnel understand their role within ABC-CA and that they are suitable for the role assigned.

Line managers/senior management are responsible to ensure personnel under their supervision apply all necessary security requirements in accordance with established policies and procedures.

Terminations of employment follow ABC-CA's 'Disciplinary Procedure.' Any changes to, or termination of employment, must be advised to the required 'Systems Administrators' to ensure the correct access rights are granted, modified or revoked as necessary.

All ABC-CA personnel, regardless of their position or role, are responsible for conducting their work in a manner that safeguards the protection of information (internal and external) within ABC-CA. All employees are advised of their responsibility for adhering to the Information Security Policy. The Information Security Policy sets out the means of protecting, preserving and managing the confidentiality, integrity and availability of not only information but also all supported business systems, processes and applications.

Supporting documentation is made available to all ABC-CA employees on the Company Intranet site. Each employee is required to understand the policies and procedures relevant to their job function as part of their ongoing information security training.

Physical and Environmental Security

Systems providing online certificate issuance (e.g. Issuer CAs) are located in corporate data centers that are located in San Francisco and Toronto. The San Francisco data center is operated by QRS Data Storage, Inc. and the Toronto location is operated by XYZ Data Centers, Inc. ABC-CA has implemented controls in addition to those provided by the data center to protect online equipment (including certificate status servers and CMS equipment) from unauthorized access and implements physical controls to reduce the risk of equipment tampering. These controls include physical barriers, such as a dedicated caged environment, with two person and two factor access controls. ABC-CA has also implemented video surveillance monitoring in

Insert report restriction

addition to the services provided by the third-party data center. The data centers provide various layers of external security barriers, security personnel on duty full time (24 hours per day, 365 days per year), and environmental controls.

The data centers that house the production environment (including supporting infrastructure) are equipped with the following environmental safeguard: Fire detection and suppression devices, air conditioning system for temperature and humidity control, Uninterruptible Power Supply (UPS) devices and backup generators to provide additional time to resolve power outages.

The ABC-CA data centers are continuously attended. However, if ABC-CA ever becomes aware that a data center is to be left unattended or has been left unattended for an extended period of time, ABC-CA personnel will perform a security check of the data center to verify that:

- ABC-CA's equipment is in a state appropriate to the current mode of operation,
- Any security containers are properly secured,
- Physical security systems (e.g., door locks) are functioning properly, and
- The area is secured against unauthorized access.

ABC-CA's administrators are responsible for making these checks and must sign off that all necessary physical protection mechanisms are in place and activated. The identity of the individual making the check is logged.

ABC-CA's RA operations are protected using physical access controls making them accessible only to appropriately authorized individuals. Access to secure areas of buildings requires the use of an "access" or "pass" card. Access card use is logged by the building security system. The exterior and internal passageways of buildings are equipped with motion detecting sensors and video cameras. Access to ABC-CA's secure cage required two trusted roles to present access cards and finger prints. Access card logs and video records are reviewed on a regular basis. ABC-CA securely stores all removable media and paper containing sensitive plain-text information related to its CA operations in secure containers.

Dedicated RA office space is provided in San Francisco, Toronto, and Tokyo. RA office space requires access cards to enter and is equipped with motion-activated video surveillance cameras. The secure office space includes fire rated file cabinets to retain all hard copies of sensitive materials, as well as, secure shredding equipment. RA office spaces included dedicated secure connections to the CA services in the third-party data centers.

Operations Management

ABC-CA defines a system incident as a significant incident that impact security or service integrity issues, such as any breach of information security; that is, any event that compromises the integrity, confidentiality and availability information stored in ABC-CA's systems. All incidents are evaluated and managed based on the ABC-CA Incident Response and Compliance

Policy. During the period January 1, 20XX to December 31, 20XX, ABC-CA did not identify any system events that met the definitions as described above.

System Incidents can be identified through a manual notification or through automated alerts. Monitoring over ABC-CA's production systems (e.g., operating systems, applications, database and networks) is the responsibility of the Infrastructure Team who utilizes various tools such as Cacti, Xymon, and/or Big Brother for internal monitoring. External monitoring is also performed through independent third parties such as PeriscopeIT and Securityspace.com. Notifications and alerts are automatically presented to the Infrastructure Team through the use of web pages, graphical interfaces, emails, and SMS alerts and then escalated to core System Administrators and applicable members of Senior Management, as necessary.
All incidents, or suspected incidents, are also reported to the appropriate asset owner, or ABC-CA's Management team for investigation. As an incident could come from any area of the company, third party, or even from an automated system, an initial assessment of the incident is performed to determine the validity of the request.

Incidents are then escalated to an Incident Handler/Investigator who is responsible for conducting a detailed investigation of the incident through resolution. The investigation encompasses a detailed study of all events relating to the incident, from initial warnings received, personnel on call to systems/applications/processes affected. Details of incidents are then documented within an 'Incident Management and Handling Report' which contains the following relevant information:

- Incident Details: Incident date & time, incident handler/investigators name, asset owner/delegate;
- Executive Summary of the Incident: How the incident was detected and raised along with step by step details of what was performed in the initial investigation;
- Summary of Key Events: Summary of the key events that occurred during the investigation and resolution of the incident;
- Impact of Incident on Business Operations: Details of the impact of the incident on business operations; and
- Root Cause Analysis: Details of the root cause of the incident and how this effected business operations.

Once all relevant information has been gathered, it is the duty of the Incident Handler/Investigator and the relevant asset owner to produce a detailed post-incident review. This includes details of any solutions and/or preventative measures required to avoid any further incidents of this nature along with any changes to ABC-CA's business processes as required.

Where an incident involves a breach of any ABC-CA policy, whether it has directly or indirectly led to any actual compromised data or not, the review contains details of such breaches and any recommendations for educational or disciplinary measures.

Insert report restriction

In cases where data loss, or probable data loss, may directly impact Customers and/or partners, a suitable report is generated and distributed. This explains the source, & scale, of any data loss, any risks to data security, and, where suitable, a suggestion of steps to perform to limit potential damage. This may include advice to reset passwords, or cancel credit/debit cards etc.

System Access Management

Logical Access

User access requests to the production environment (including network, operating systems, applications and databases) are formally submitted through the use of a 'Systems Access Request Form' and approved by the appropriate line manager/senior management prior to access being granted. Users are granted privileges on systems according to their assigned roles and duties.

The Systems Administration Team or Application Owner creates or modifies accounts only upon receipt of a fully authorized 'Systems Access Request Form'. When new users are created, the System Administrator ensures that User IDs are unique.

When an employee leaves ABC-CA, the Systems Administration Team; disables all assigned accounts (across all systems), changes the user's passwords, and revokes the user's keys/certificates, as required within 24 hours. In the event of an employee being suspended, all user accounts will be disabled within 24 hours and remain disabled until the outcome of any investigations is complete.

Privileged access to the production environment (including network, operating system, applications and database layers) is limited to authorized administrators based on current roles and responsibilities. The process for granting and removing privileged access follows ABC-CA's user administration process and requires approval from the administrator's manager.

Password configuration rules have been implemented across all layers of technology (where technology permits) based on ABC-CA's logical access policies. These configuration rules include forced password change upon initial log-on, maximum password age, minimum password length, history, account lockout duration and threshold, masked passwords, complexity, and workstation screen saver passwords. Additionally, ABC-CA displays a general notice warning that computers should only be accessed by authorized users and logging of successful and unsuccessful log-on attempts are recorded and maintained for a minimum of 30 days.

In order to confirm ABC-CA's systems are being used by authorized employees and access restrictions are appropriately assigned, reviews of user access are carried out on a quarterly basis.

Insert report restriction

Network Security

Access to ABC-CA's network and the related network devices (e.g., routers, switches, etc.) is restricted to employees whose job responsibilities require them to have such access. User access requests to the network and related assets are formally submitted and approved by an ABC-CA manager prior to access being granted.

There is no remote access permitted to the air gapped network in the secure zone. Remote access to the remaining ABC-CA network is protected and secured through encrypted VPN tunnels from ABC-CA's locations. HTTPS authentication to the network requires a variation of valid User IDs, passwords, certificates, and/or USB token/smart cards. Encrypted VPN access is available to users on a “needs” basis and is protected by USB token certificates generated for that purpose.

Firewall devices are installed within ABC-CA’s network to filter and segregate internal and external network traffic. ABC-CA’s network is segregated based on the information services they support.

Windows desktops have Anti-Virus products installed that are monitored by the Infrastructure Team for virus attacks. Desktops with Linux-based operating systems have various methods of mitigating virus/malware threats, such as root kit detection software, hardened tool chains and hardened kernels. In addition, email servers have Anti-Virus software installed to prevent infection from email. These signature files are updated on a regular basis (every 2 hours). Emails are scanned as mail passes through the mail servers, i.e., scanning is applied during ingress and egress processes. All desktops are located behind firewalls that block ports that are known vectors of attack. Servers having Linux based operating systems also have methods for mitigating virus/malware threats that include, but are not limited to, installation of root kit detection software, hardened tool chains, and hardened kernels.

Physical Access

General

Access to the ABC-CA data centers as well as business offices (located in the same locations as data centres), is protected through physical security barriers that require a variation of biometric, key/key fob and key card access for entry. In addition to these access control mechanisms, video cameras have been deployed in strategic locations inside and outside each of the data centers and security guards are present at the main building entrances for further protection.

Access to the ABC-CA data centers is restricted to authorized employees and other approved individuals (e.g., visitors) who require this level of access to perform their job responsibilities. Access is recorded from electronic badging or, for visitors, filling in information on a visitor log that is maintained in the secure zone.

Requests for access to the data centers require completion of a 'Data Center Access Request form' and approval from relevant IT Management. Visitors gaining access to the data centers must wear a badge and are also required to be escorted by at least one ABC-CA employee at all times.

When an employee leaves ABC-CA, the CIO, or delegate, will advise access revocation within 24 hours. In the event of an employee being suspended, the employee's data center access will be disabled within 24 hours and remain disabled until the outcome of any investigations is complete.

Secure Zone

All ABC-CA PKI equipment located at the data centers is housed in secure locked cabinets in the secure zone. Access to these cabinets is only available to authorized ABC-CA personnel under dual custody access, or authorized data center staff that provide support. Video cameras monitor activity in PKI cages on 24 by 7 basis.

The biometric authentication access systems log each use of the access card. Activation data must either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module. Activation data is never stored with the cryptographic module or removable hardware. Cryptographic hardware includes a mechanism to lock the hardware after a certain number of failed login attempts.

Cryptomodule activation keys (operator cards and PED keys) are either sealed in tamper-evident bags and placed in safe deposit boxes or stored in the two-person safe in the secure zone when not in use. Access to the safe is manually logged. Access card logs and the manual logs of access to the safe are reviewed on a regular basis.

Systems Development, Maintenance, and Change Management

Changes to the production environment within ABC-CA originate from a variety of sources, including information owners, system owners, project/Infrastructure teams, and Customers and are categorized into one of the following:
F

- Implementation of a New System or Business Process – A new release of an information system or the implementation of a new business process that provides new or/and enhanced functionality (project driven).
- Problem with an IT System/Business Process or a Security Incident – Fixing a user identified system defect that is impacting service delivery or patching a system to address a newly identified security vulnerability (incident driven).
- Preventative Maintenance – Applying routine system patches and standard upgrades.
- Application Development – includes development of a new application or significant changes to an existing code base and follows a formal process for testing and approvals.

Change requests are documented using a 'Change Request Form' that contains all required details of the change and is used from initial request to final production deployment. Changes are classified as Normal, Pre-Approved or Emergency. The majority of changes fall into the Normal classification. The Emergency classification is only used for an incident driven problem to fix a critical issue in a critical business system. Pre-approved changes consist of standardized, low risk, or routine related changes such as server patches and routine server restarts.

Change requests are submitted to the Asset Owner, who assess the request by capturing the necessary requirements and the possible impact on ABC-CA's business/systems. Asset Owner/Project Managers are then responsible for reviewing and authorizing change requests and assigning a developer.

Once the development of the change is complete, testing is performed dependent on the nature of the change to confirm the changes align with the request and the change does not have a negative impact on the overall security within the systems. Testing may be performed against data within the development environment, System Administrators and, in some cases business users, may be asked to perform user acceptance testing within the test environment. If testing is successful, the responsible tester provides a sign-off that testing is complete and changes are ready to be migrated to production. If testing is un-successful, the change is re-developed until corrected.

Change requests ready for production migration undergo pre-deployment verification and a risk assessment to determine the impact of the change on the production environment which is completed by the Asset Owner/Project Manager. The risk assessment decision will be made based on the category to which the change is classified. All changes must have fully documented development, pre-deployment testing, and defined regression plans before being deployed to the

production environment. Once completed, changes are then approved by the Asset Owner/Management for migration to production.
Approved change requests are then scheduled for deployment to the production environment by a segregated group of individuals from the development team and based on their business requirements and impact by the Asset Owner and/or Project Manager.

Post deployment testing is performed to determine if the change was successful and meets expectations. Should any of the tests fail, the change may either remain in place with further rework or undergo the regression plan to be rolled back.

Responsibilities of personnel within ABC-CA are organized so that it is not possible for one person to develop, test, authorize and migrate a change to the production environment, infrastructure or data. Personnel in systems development may not authorize code changes to the production environment or sign-off testing.

Disaster Recovery, Backups, and Business Continuity Management

Disaster Recovery and Business Continuity
ABC-CA has robust, regularly tested Business Continuity and Disaster Recovery Plans, to help ensure the timely resumption of business activities and critical business processes from the effects of major failures of information systems or disasters.

ABC-CA accepts that business continuity is very much dependent on the design of the processes and systems running business critical applications and services. As a result, ABC-CA operates a 'Preventative Policy' for business continuity in that all primary business critical processes, systems, applications and operations are designed in such a way as to prevent predictable, and minimize the impact of unpredictable events. Access to said systems and applications is also governed by the principle that all access is denied unless explicitly authorized by management.

ABC-CA attempts to reduce the risk of a major event compromising business operations by defining four levels of redundancy as detailed below:

Device Level
Critical hardware resources required for machines are configured in 'fault tolerant mode'. Single point of failure is averted. For example, Dual PSU, Multiple hard disk drives in a RAID configuration, multiple network interfaces in bridged mode.

Machine Level
Machines providing Critical services at the data center sites are replicated and configured as master and slave, thereby providing fail-over in case a machine providing a service becomes inoperable.

City Level
Critical services are replicated across multiple data center sites that are available in geographically separate locations but in the same country. If one of the sites becomes unreachable due to a natural or man-made disaster, business can be continued from the alternate site(s).

Country Level
At least one of the data center sites is geographically located in another country. If there were to be a country-wide disaster affecting all of the data center sites in one country, business can be continued from an alternative data center site located in another country.
The minimum hardware redundancy standard is as follows:

- Redundant Power supplies to a minimum level of N+1
- Redundant Network Connections
- Hard Drive Redundancy (RAID)
- Infrastructure Redundancy to a level of N+1

The offices in which ABC-CA operates its business are critical to business operations for back office processing, product & business development and business management. To guard against the loss of office operations, whether this is caused by power failure, natural disaster, fire, theft etc., ABC-CA operates offices based across multiple sites and geographical locations. All office locations operated by ABC-CA are 'fit for purpose' and comply with ABC-CA's requirements for physical security.

The back-office processing activity may be carried out from anywhere with Internet connectivity, since the interface is a publicly available web interface. The security of this interface is ensured by having it only available over SSL and requiring identification by means of an SSL Client certificate and authentication by means of username and password.

In the normal course of events, “back office processing” is carried out from ABC-CA’s San Francisco and Toronto offices. It is conceivable that any of those offices could lose Internet connectivity or mains power, rendering the normal back office processing facility from that location inoperative. In the event of a loss of an office location, local management personnel will inform ABC-CA's Operations Managers (or delegates) of the event along with all relevant details, e.g. cause, estimated time for resumption, systems and operations effected etc. From these details the Operations Manager, in discussion with relevant management personnel, shall decide upon, and implement a recovery operation

Backups

Servers within the production system are backed-up according to a predefined schedule. The schedule performs a daily local backup of all running servers (physical and virtual) that is stored, via an encrypted network connection, on a server located in the local data center. On a weekly

basis, the local backup servers execute a sync that pushes the backups from the local backup server to an encrypted file system on a backup server located at the Bradford data center using Secure Shell (SSH) over an encrypted network connection (VPN/GRE). The encrypted file system at the Bradford location employs a block device-layer disk encryption system specification.

In addition to local & off-site backups, the servers themselves form high availability pairs. That is, complete duplicates of servers that become active if its partner suffers failure. Though not conventional backup in the classical sense, it represents another copy of a given host that can be used to restore any failed hosts. High availability is configured through DRBD (Distributed Replicated Block Device) and Heartbeat.

Database backups are continuously replayed to the standby server at the live site and also to servers at the standby sites after allowing a time delay for corruption prevention. Off-site backups are also pushed to the backup server located at the Bradford data center.

System/Database Administrators at each ABC-CA data center location are responsible for carrying out and maintaining scheduled backup activities. Scheduled backups are automated using approved backup tools and transferred using secure methods. ABC-CA utilizes a number of different types of backup media, including compact discs, digital versatile disks and hard disk drives, to best suit the backup application.
Unscheduled backups of pertinent data occur before carrying out major changes to business-critical systems. Unscheduled backup activities are coordinated between information owners and the System Administrators.

The scheduled backup process of business-critical systems and applications is monitored using automated tools. In the event of a backup failing, an alert is emailed to the Infrastructure Team or the Database Administrator. These alerts are then investigated and resolved as a matter of high priority. Only System Administrators have the ability to make changes to the back-up scheduling tool.

Monitoring and Compliance

Certificate Audits
[Insert client specific information]

Access Reviews
[Insert client specific information]

Compliance Reviews
[Insert client specific information]

Insert report restriction

System Monitoring
[Insert client specific information]

Audit Logging

Logging
[Insert client specific information]

Retention
[Insert client specific information]

Principle 4 – CA Key Lifecycle Management Controls

CA Key Generation

CA key generation and signing occurs either in the secure storage room or in a room of commensurate security in close proximity thereto. ABC-CA's CA Administrators retrieve cryptographic materials necessary to perform key generation and certificate signing. At no time are cryptographic materials left unattended by fewer than two persons serving in trusted roles.

In the Secure Zone the following equipment is used (discuss as appropriate, whether air gapped etc.):

- Type of computer/servers
- Locked cabinets – dual custody
- Cameras
- Type of HSMs
- Safe

CA Key Storage, Backup, and Recovery

ABC-CA securely stores the cryptomodules used to generate and store offline CA Private Keys in the San Francisco and Toronto offices. Access to the rooms used for key storage is controlled and logged by the building access card system. When not in use during a key ceremony, CA cryptomodules are locked in a safe that provides two-person physical access control. Cryptomodule activation keys (operator cards and PED keys) are either sealed in tamper-evident bags and placed in safe deposit boxes or stored in the two-person safe when not in use. Access to the safe is manually logged. Access card logs and the manual logs of access to the safe are reviewed on a regular basis.

CA Key Public Distribution
[Insert client specific information]

Insert report restriction

CA Key Usage
[Insert client specific information]

CA Key Archival
[Insert client specific information]

CA Key Destruction
[Insert client specific information]

CA Key Compromise
[Insert client specific information]

CA Cryptographic Hardware Life Cycle Management
[Insert client specific information]

CA Key Transportation
[Insert client specific information]

CA Key Migration (if applicable)
[Insert client specific information]

Principle 5 – Subscriber Key Lifecycle Controls

CA-Provided Subscriber Key Generation Services
[Insert client specific information]

CA-Provided Subscriber Key Storage and Recovery Services
[Insert client specific information]

Integrated Circuit Card (ICC) Lifecycle Management
[Insert client specific information]

Requirements for Subscriber Key Management
[Insert client specific information]

Principle 6 – Certificate Lifecycle Management

Subscriber Registration
[Insert client specific information]

Certificate Renewal

[Insert client specific information]

Certificate Rekey
[Insert client specific information]

Certificate Issuance
[Insert client specific information]

Certificate Distribution
[Insert client specific information]

Certificate Revocation
[Insert client specific information]

Certificate Validation
[Insert client specific information]

Principle 7 – Subordinate CA and Cross Certificate Lifecycle Management Controls

Subordinate CA Certificate and Cross Certificate Lifecycle Management
[Insert client specific information]

Attachment 1 – List of CAs in Scope

CA #	Cert #	Subject	Issuer	Serial	Not Before	Not After	SKI
1	1	C=CA O=ABC-CA Inc. CN=ABC-CA Root CA – G1	C=CA O=ABC-CA Inc. CN=ABC-CA Root CA – G1	6D5A334C1BAF569E	Mar 13 17:13:04 2017 GMT	Dec 31 17:13:04 2030 GMT	02:AE:95:D6:52:E5:01:87:40:AD:11:AF:DC:CD:01:EE:69:A4:77
2	1	C=CA O=ABC-CA Inc. CN=ABC-CA Issuing CA – EV	C=CA O=ABC-CA Inc. CN=ABC-CA Root CA – G1	7DAAAF3CF15F8F45	Mar 14 01:25:41 2017 GMT	Mar 14 01:25:41 2027 GMT	92:A4:60:D4:ED:AC:57:3D:C2:1B:24:07:0D:AF:AC:DD:F1:8A:9A
2	2	C=CA O=ABC-CA Inc. CN=ABC-CA Issuing CA – EV	C=CA O=ABC-CA Inc. CN=ABC-CA Root CA – G1	8FABAF6CF45F884F	Apr 22 07:41:53 2017 GMT	Apr 22 07:41:53 2027 GMT	92:A4:60:D4:ED:AC:57:3D:C2:1B:24:07:0D:AF:AC:DD:F1:8A:9A

CAs Revoked During the Period

Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Date Revoked	SHA256 Fingerprint
C=CA O=ABC-CA Inc. CN=ABC-CA Root CA – G1	C=CA O=ABC-CA Inc. CN=ABC-CA Root CA – G1	6D5A334C1BAF569E	rsaEncryption	(4096 bit)	sha256WithRSAEncryption	Mar 13 17:13:04 2017 GMT	DB:AF:00:71:06:47:95:A5:78:I
C=CA O=ABC-CA Inc. CN=ABC-CA Issuing CA – EV	C=CA O=ABC-CA Inc. CN=ABC-CA Root CA – G1	7DAAAF3CF15F8F45	rsaEncryption	(2048 bit)	sha256WithRSAEncryption	Mar 14 01:25:41 2017 GMT	DF:30:CF:75:83:21:F7:F6:D0:(

Section 4

Independent WebTrust Practitioner's Description of Tests of Controls and Results Thereof

The following has been drafted using the Illustrative controls have been included with each WebTrust Criterion in WebTrust for CA to provide guidance to CAs and auditors on the types of controls that should be evaluated to achieve each criterion. In addition, since this report will likely only be used by A CA that is part of a trusted root program, the relevant criteria from the WebTrust Baseline and Network Security have been included. The sample controls included in those sections are based on either the requirements of the CA Browser Forum or other sample controls that were developed by the Task Force. They are not designed to be either complete or exhaustive in nature.

Independent Service Auditor's Description of Tests of Controls and Results

This report is intended to provide information to the management of ABC-CA and user entities of the ABC-CA Certification Authorities System, who have a sufficient understanding to consider it, along with other information including information about the controls implemented by the user entity. This report is intended to provide information about the suitability of the design and operating effectiveness of the controls implemented to meet the WebTrust for Certification Authorities Criteria, and the WebTrust Principles And Criteria For Certification Authorities –SSL Baseline With Network Security set forth by CPA Canada at [insert current CPA Canada link] *)* ("applicable WebTrust criteria"), throughout the period January 1, 20XX to December 31, 20XX.

The examination was performed in accordance with the Description criteria set forth by CPA Canada in [insert document name and location]

This description is intended to focus on ABC-CA's controls surrounding the ABC-CA Certification Authorities System throughout the period January 1, 20XX to December 31, 20XX; it does not encompass all aspects of the services provided or controls performed by ABC-CAs. Unique processes or control situations not described in the report are outside the scope of this report.

Tests of Controls

Our examination of the description of the ABC-CA's ABC-CA Certification Authorities System and the suitability of the design and operating effectiveness of the controls to achieve the related control criteria stated in the description involved performing procedures to obtain evidence about the fairness of the presentation of the description of the system and the suitability of the design and operating effectiveness of those controls to achieve the related control criteria stated in the description. Our procedures included assessing the risks that the description is not fairly

presented and that the controls were not suitably designed or operating effectively to achieve the related control criteria stated in the description.

Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control criteria stated in the description were achieved throughout the period January 1, 20XX to December 31, 20XX.

Our testing of controls was restricted to the controls specified by ABC-CA's in Section 4, and was not extended to controls in effect at user locations or other controls which were not documented as tested under each control criteria listed in Section IV. The description of our tests of controls and results of those tests are presented in this section of the report. The description of the tests of controls and the results of those tests are the responsibility of firm name, LLP and should be considered information provided by firm name LLP.

Type	Description
Inquiry	Made inquiries of appropriate personnel and corroborated responses with management.
Observation	Observed the application or existence of the specific control(s) as represented by management.
Inspection	Inspected documents and records indicating performance of the control. This includes examples such as: • Inspection of audit evidence that demonstrate the performance of the control. • Inspection of systems documentation, for example operations manuals, flow charts and job descriptions. • Reading documents such as policies and meeting minutes to determine appropriate information is included.
Reperformance	Reperformed the control or processing application to ensure the accuracy of its operation. This includes examples such as: • Obtaining evidence of the arithmetical accuracy and correct processing of transaction by performing independent calculations. • Processing test transactions through application programs in a test environment. • Reperforming the matching of various system records by independently matching the same records and comparing reconciling items to prepared reconciliations.

WebTrust Principles, Criteria, Related Controls and Tests of Controls

Criteria Related to CA Business Practices Disclosure

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
1.1	**WebTrust for CA Criteria** - The CA discloses its business practices including but not limited to the topics listed in RFC 3647 or RFC 2527 in its Certification Practice Statement.		
1.2	**WebTrust for CA Criteria** - The CA discloses its business practices including but not limited to the topics listed in RFC 3647 or RFC 2527 in its Certificate Policy.		

Criteria related to CA Business Practices Management

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
2.1	**WebTrust for CA Criteria -** The CA maintains controls to provide reasonable assurance that its Certification Practice		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	Statement (CPS) management processes are effective.		
	1) The PA has final authority and responsibility for approving the CA's Certification Practice Statement (CPS). 2) Responsibilities for maintaining the CPS have been formally assigned. 3) The CA's CPS is modified and approved in accordance with a defined review process. 4) The CA makes available its Certification Practice Statement (CPS) to all appropriate parties. 5) Revisions to the CA's CPS are made available to appropriate parties. 6) The CA updates its CPS to reflect changes in the environment as they occur.		
2.2	**WebTrust for CA Criteria -** The CA maintains controls to provide reasonable assurance that its Certificate Policy (CP) management process is effective		
	1) The Policy Authority (PA) has the responsibility of defining the business requirements and policies for using digital certificates and specifying them in a Certificate Policy (CP) and supporting agreements. 2) The PA has final authority and responsibility for specifying and approving Certificate Policy(s). 3) Certificate Policy(s) are approved by the Policy Authority in accordance with a defined annual review process, including responsibilities for maintaining and tracking changes to the Certificate Policy(s).		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	4) A defined review process exists to assess that the Certificate Policy(s) are capable of support by the controls specified in the CPS. 5) The PA makes available the Certificate Policies supported by the CA to Subscribers and Relying Parties.		

Criteria Related to CP and CPS Consistency (if applicable)

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
2.3	**WebTrust for CA Criteria -** The CA maintains controls to provide reasonable assurance that its Certification Practice Statement addresses the topics included in its Certificate Policy.		
	1) The PA is responsible for ensuring that the CA's control processes, as stated in a Certification Practice Statement (CPS) or equivalent, fully comply with the requirements of the CP. 2) The CA addresses the requirements of the CP when developing its CPS. 3) The CA assesses the impact of proposed CPS changes to ensure that they are consistent with the CP. 4) A defined review process exists to ensure that Certificate Policy(s) are supported by the CA's CPS.		

Criteria Related to CA Environmental Controls

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	Security Management		
3.1	**WebTrust for CA Criteria -** The CA maintains controls to provide reasonable assurance that: • security is planned, managed and supported within the organisation; • security risks are identified and managed; • the security of CA facilities, systems and information assets accessed by third parties is maintained; and • the security of subscriber and relying party information is maintained when the responsibility for CA sub-functions has been outsourced to another organisation or entity.		
	Information Security Policy 1) An information security policy document, that includes physical, personnel, procedural and technical controls, is approved by management, published and communicated to all employees. 2) Responsible management of the CA demonstrates that the information security policy is implemented and adhered to. 3) The information security policy includes the following: a) a definition of information security, its overall objectives and scope, and the importance of security as an enabling mechanism for information sharing;		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	b) a statement of management intent, supporting the goals and principles of information security; c) an explanation of the security policies, principles, standards and compliance requirements of particular importance to the organisation; d) a definition of general and specific responsibilities for information security management, including reporting security incidents; and e) references to documentation, which supports the policy. 4) There is a defined review process for maintaining the information security policy, including responsibilities and review dates.		
	Information Security Infrastructure 5) Senior management and/or a high-level management information security committee have the responsibility to ensure there is clear direction and management support to manage risks effectively. 6) A management group or security committee exists to co-ordinate the implementation of information security controls and the management of risk. 7) Responsibilities for the protection of individual assets and for carrying out specific security processes are clearly defined. 8) A management authorisation process for new information processing facilities exists and is followed.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	Security of Third-Party Access 9) Procedures exist and are enforced to control physical and logical access to CA facilities and systems by third parties (e.g., on-site contractors, trading partners and joint ventures). 10) If there is a business need for the CA to allow third party access to CA facilities and systems, a risk assessment is performed to determine security implications and specific control requirements. 11) Arrangements involving third party access to CA facilities and systems are based on a formal contract containing necessary security requirements.		
	Outsourcing 12) If the CA outsources the management and control of all or some of its information systems, networks, and/or desktop environments, the security requirements of the CA are addressed in a contract agreed upon between the parties. 13) If the CA chooses to delegate a portion of the CA roles and respective functions to another party, the CA maintains responsibility for the completion of the outsourced functions and the definition and maintenance of a statement of its CPS.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	Asset Classification and Management		
	WebTrust for CA Criteria - The CA maintains controls to provide reasonable assurance that CA assets and subscriber and relying party information receive an appropriate level of protection based upon identified risks and in accordance with the CA's disclosed business practices.		
3.2	1) Owners are identified for all CA assets and assigned responsibility for the protection of the assets. 2) Inventories of CA assets are maintained. 3) The CA has implemented information classification and associated protective controls for information based on business needs and the business impacts associated with such needs. 4) Information labelling and handling are performed in accordance with the CA's information classification scheme and documented procedures.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	Personnel Security		
3.3	**WebTrust for CA Criteria** - The CA maintains controls to provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	1) The CA employs personnel (i.e., employees and contractors) who possess the relevant skills, knowledge and experience required for the job function.		
	2) Security roles and responsibilities, as specified in the organisation's security policy, are documented in job descriptions.		
	3) Trusted Roles, on which the security of the CA's operation is dependent, are clearly identified. Trusted roles include, at a minimum, the following responsibilities: a) overall responsibility for administering the implementation of the CA's security practices; b) approval of the generation, revocation and suspension of certificates; c) installation, configuration and maintenance of the CA systems; d) day-to-day operation of CA systems and system backup and recovery; e) viewing and maintenance of CA system archives and audit logs; f) cryptographic key life cycle management functions (e.g., key component custodians); and g) CA systems development.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	4) The CA's policies and procedures specify the background checks and clearance procedures required for Trusted Roles and non-trusted roles. As a minimum, verification checks on permanent staff are performed at the time of job application and periodically for those individuals undertaking Trusted Roles.		
	5) An individual's trusted status is approved prior to gaining access to systems/facilities or performing actions requiring trusted status.		
	6) CA Employees and Trusted Roles sign a confidentiality (non-disclosure) agreement as a condition of employment.		
	7) Contractors who perform Trusted Roles are subject to at least the same background check and personnel management procedures as employees.		
	8) Any contract arrangement between Contractors and CAs allows for the provision of temporary contract personnel that explicitly allows the organisation to take measures against contract staff who violate the organisation's security policies. Protective measures may include: a) bonding requirements on contract personnel;		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	b) indemnification for damages due to contract personnel wilful harmful actions; and c) financial penalties.		
	9) Periodic reviews occur to verify the continued trustworthiness of personnel involved in the activities related to key management and certificate management.		
	10) A formal disciplinary process exists and is followed for employees who have violated organisational security policies and procedures. The CA's policies and procedures specify the sanctions against personnel for unauthorised actions, unauthorised use of authority, and unauthorised use of systems.		
	11) Physical and logical access to CA facilities and systems is disabled upon termination of employment.		
	12) If required based on a risk assessment, duress alarms are provided for users who might be the target of coercion.		
	13) All employees of the organisation and, where relevant, third party contractors, receive appropriate training in organisational policies and procedures. The CA's policies and procedures specify the following:		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	a) The training requirements and training procedures for each role; and b) Any retraining period and retraining procedures for each role.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	Physical and Environmental Security		
	CA Facility Physical Security		
3.4	**WebTrust For CA Criteria -** The CA maintains controls to provide reasonable assurance that: • physical access to CA facilities and equipment is limited to authorised 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.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	1) Entry to the building or site containing the CAs certificate manufacturing facility is achieved only through a limited number of controlled access points.		
	2) All critical CA operations take place within a physically secure facility with at least four layers of security to access sensitive hardware or software. Such systems are physically separated from the organisation's other systems so that only authorised employees of the CA can access them.		
	3) A manned reception area or other means to control physical access is in place to restrict access to the building or site housing CA operations to authorised personnel only.		
	4) Physical barriers are in place (e.g., solid walls that extend from real floor to real ceiling) to prevent unauthorised entry and environmental contamination to the CAs certificate manufacturing facility.		
	5) Physical barriers are in place (e.g., Faraday cage) to prevent electromagnetic radiation emissions for all Root CA operations (e.g., key generation and certification of CA Certificates) as disclosed in CP and/or CPS.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	6) Fire doors exist on security perimeters around CA operational facilities and are alarmed and conform to local fire regulations.		
	7) Intruder detection systems are installed and regularly tested to cover all external doors of the building housing the CA operational facilities.		
	8) CA operational facilities are physically locked and alarmed when unoccupied.		
	9) All personnel are required to wear visible identification. Employees are encouraged to challenge anyone not wearing visible identification.		
	10) Access to CA operational facilities is controlled and restricted to authorised persons through the use of multi-factor authentication controls.		
	11) All personnel entering and leaving CA operational facilities are logged (i.e., an audit trail of all access is securely maintained).		
	12) Entry, exit, and activities within CA facilities are monitored by cameras.		
	13) Visitors to CA facilities are supervised and their date and time of entry and departure recorded.		
	14) Third party support services personnel is granted restricted		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	access to secure CA operational facilities only when required and such access is authorised and accompanied.		
	15) Access rights to CA facilities are regularly reviewed and updated.		
	Equipment Security		
	16) The CA maintains an equipment inventory.		
	17) Equipment is sited or protected such as to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.		
	18) Equipment is protected from power failures and other electrical anomalies.		
	19) Power and telecommunications, within the facility housing the CA operation, cabling carrying data or supporting CA services is protected from interception or damage.		
	20) Equipment is maintained in accordance with the manufacturer's instructions and/or other documented procedures.		
	21) All items of equipment containing storage media (fixed and removable disks) are checked to ensure that they do not contain sensitive data prior to their disposal. Storage media		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	containing sensitive data is physically destroyed or securely overwritten prior to disposal or reused.		
	General Controls		
	22) Sensitive or critical business information is locked away when not required and when the CA facility is vacated.		
	23) Procedures require that personal computers and workstations are logged off or protected by key locks, passwords or other controls when not in use.		
	24) The movement of materials to/from the CA facility requires prior authorisation.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	Operations Management		
	Operational Procedures and Responsibilities		
3.5	**WebTrust for CA Criteria -** The CA maintains controls to provide reasonable assurance that: • the secure operation of CA information processing facilities is ensured; • the risk of CA systems failure is minimised;		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	• the integrity of CA systems and information is protected against viruses and malicious software; • damage from security incidents and malfunctions is minimised through the use of incident reporting and response procedures; and media are securely handled to protect them from damage, theft and unauthorised access.		
	1) CA operating procedures are documented and maintained for each functional area.		
	2) Formal management responsibilities and procedures exist to control all changes to CA equipment, software and operating procedures.		
	3) Duties and areas of responsibility are segregated in order to reduce opportunities for unauthorised modification or misuse of information or services.		
	4) Development and testing facilities are separated from operational facilities.		
	5) Prior to using external facilities management services, risks and related controls are identified, agreed upon with the contractor, and incorporated into the contract.		
	System Planning and Acceptance		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	6) Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.		
	7) Acceptance criteria for new information systems, upgrades and new versions are established and suitable tests of the system carried out prior to acceptance		
	Protection Against Viruses and Malicious Software		
	8) Detection and prevention controls to protect against viruses and malicious software, including on offline or air gapped systems are implemented. Employee awareness programs are in place.		
	Incident Reporting and Response		
	9) A formal security incident reporting procedure exists setting out the actions to be taken on receipt of an incident report. This includes a definition and documentation of assigned responsibilities and escalation procedures. Any incidents are reported to responsible management as a matter of urgency.		
	10) Users of CA systems are required to note and report		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	observed or suspected security weaknesses in, or threats to, systems or services as they are detected.		
	11) Procedures exist and are followed for reporting hardware and software malfunctions.		
	12) Procedures exist and are followed to assess that corrective action is taken for reported incidents.		
	13) A formal problem management process exists that allows the types, volumes and impacts of incidents and malfunctions to be documented, quantified and monitored.		
	Media Handling and Security		
	14) Procedures for the management of removable computer media require the following: a) if no longer required, the previous contents of any reusable media that are to be removed from the organisation are erased or media is destroyed; b) authorisation is required for all media removed from the organisation and a record of all such removals to maintain an audit trail is kept; and c) all media are stored in a safe, secure environment, in accordance with		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	manufacturers' specifications.		
	15) Equipment containing storage media (i.e., fixed hard disks) is checked to determine whether they contain any sensitive data prior to disposal or reuse. Storage devices containing sensitive information are physically destroyed or securely overwritten prior to disposal or reuse.		
	16) Procedures for the handling and storage of information exist and are followed in order to protect such information from unauthorised disclosure or misuse.		
	17) System documentation is protected from unauthorised access.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	System Access Management		
	User Access Management		
3.6	**WebTrust for CA Criteria-** The CA maintains controls to provide reasonable assurance that CA system access is limited to authorised individuals. Such controls provide reasonable assurance that:		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	• hypervisor, operating system, database, and network device access is limited to authorised individuals with predetermined task privileges; • access to network segments housing CA systems is limited to authorised individuals, applications and services; and • CA application use is limited to authorised individuals.		
	1) Business requirements for access control are defined and documented in an access control policy that includes at least the following: a) roles and corresponding access permissions; b) identification and authentication process for each user; c) segregation of duties; and d) number of persons required to perform specific CA operations (i.e., m of n rule where m represents the number of key shareholders required to perform an operation and n represents the total number of key shares).		
	2) There is a formal user registration and de-registration procedure for access to CA information systems and services, including hypervisors, operating systems, database, and network devices.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	3) The allocation and use of privileges is restricted and controlled.		
	4) The allocation of passwords and multi-factor authentication tokens is controlled through a formal management process.		
	5) Access rights for users with trusted roles are reviewed at regular intervals and updated.		
	6) Users are required to follow defined policies and procedures in the selection and use of passwords.		
	7) Users are required to ensure that unattended equipment has appropriate protection.		
	8) Where technically feasible, administrative and superuser accounts require the use of multifactor authentication controls.		
	Network Access Control		
	9) CA employed personnel are provided direct access only to the services that they have been specifically authorised to use. The path from the user terminal to computer services is controlled.		
	10) Remote access to CA systems, made by CA employees or external systems, if permitted, requires authentication.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	11) Connections made by CA employees or CA systems to remote computer systems are authenticated.		
	12) Access to diagnostic ports is securely controlled.		
	13) Controls (e.g., firewalls) are in place to protect the CA's internal network domain from any unauthorised access from any other domain.		
	14) Controls are in place to limit the network services (e.g., HTTP, FTP, etc.) available to authorised users in accordance with the CA's access control policies. The security attributes of all network services used by the CA organisation are documented by the CA.		
	15) Routing controls are in place to ensure that computer connections and information flows do not breach the CA's access control policy.		
	16) The CA maintains local network components (e.g., firewalls and routers) in a physically secure environment and audits their configurations periodically for compliance with the CA's configuration requirements.		
	17) Sensitive data is encrypted when exchanged over public or untrusted networks.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	Hypervisor, Operating System, Database, and Network Device Access Control		
	18) Hypervisors, operating systems, databases, and network devices are configured in accordance with the CA's system configuration standards and periodically reviewed and updated.		
	19) Hypervisors, operating system, database, and network device patches and updates are applied in a timely manner when deemed necessary based on a risk assessment and follow formal change management procedures (see § 3.7).		
	20) Automatic terminal identification is used to authenticate connections to specific locations and to portable equipment.		
	21) Access to CA systems requires a secure logon process.		
	22) All CA personnel users have a unique identifier (user ID) for their personal and sole use so that activities can be traced to the responsible individual. Where shared or group accounts are required, other monitoring controls are implemented to maintain individual accountability.		
	23) Uses of system utility programs are restricted to authorised		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	personnel and tightly controlled.		
	24) Inactive terminals serving CA systems require re-authentication prior to use.		
	25) Restrictions on connection times are used to provide additional security for high-risk applications.		
	26) Sensitive data is protected against disclosure to unauthorised users.		
	Application Access Control		
	27) Access to information and application system functions is restricted in accordance with the CA's access control policy.		
	28) CA personnel are successfully identified and authenticated before using critical applications related to certificate management.		
	29) Sensitive systems (e.g., Root CA) require a dedicated (isolated) computing environment.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	Systems Development, Maintenance, and Change Management		
3.7	**WebTrust for CA Criteria** - The CA maintains controls to provide reasonable assurance that CA systems development, maintenance		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	activities, patching, and changes to CA systems including hypervisors (where applicable), operating systems, databases, applications, network devices, and hardware are documented, tested, authorised, and properly implemented to maintain CA system integrity		
	1) Business requirements for new systems, or enhancements to existing systems specify the control requirements.		
	2) Software testing and change control procedures exist and are followed for the implementation of software on operational systems including scheduled software releases, modifications, patches, and emergency software fixes.		
	3) Change control procedures exist and are followed for the hardware, network component, and system configuration changes.		
	4) Test data is protected and controlled.		
	5) Control is maintained over access to program source libraries.		
	6) Application systems are reviewed and tested when operating system changes occur.		
	7) The implementation of changes is strictly controlled by the use of formal change control procedures to minimise the risk		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	of corruption of information systems.		
	8) Modifications to software packages are discouraged and all changes are strictly controlled.		
	9) The purchase, use and modification of software are controlled and checked to protect against possible covert channels and Trojan code. This includes the authentication of the source of the software. These controls apply equally to outsourced software development.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	Disaster Recovery, Backups, and Business Continuity Management		
3.8	**WebTrust for CA Criteria** - The CA maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster or other type of business interruption. Such controls include, at a minimum: • the development and testing of a CA business continuity plan that includes a disaster recovery process for critical components of the CA system; • the storage of required cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	• creating backups of systems, data, and configuration information at regular intervals in accordance with the CA's disclosed business practices, and storage of these backups at an alternate location; and • the availability of an alternate site, equipment and connectivity to enable recovery. The CA maintains controls to provide reasonable assurance that potential disruptions to Subscribers and Relying Parties are minimised as a result of the cessation or degradation of the CA's services.		
	1) The CA has a managed process for developing and maintaining its business continuity plans. The CA has a business continuity planning strategy based on an appropriate risk assessment.		
	2) The CA has a business continuity plan to maintain or restore the CA's operations in a timely manner following interruption to, or failure of, critical CA processes. The CA's business continuity plan addresses the following: a) the conditions for activating the plans; b) emergency procedures; c) fall-back procedures; d) resumption procedures; e) a maintenance schedule for the plan;		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	f) awareness and education requirements; g) the responsibilities of the individuals; h) recovery time objective (RTO) and recovery point objective (RPO); and i) regular testing of contingency plans.		
	3) The CA's business continuity plans include disaster recovery processes for all critical components of a CA system, including the hardware, software and keys, in the event of a failure of one or more of these components. Specifically: a) cryptographic devices used for storage of backup CA private keys are securely stored at an off-site location in order for the CA to recover in the event of a disaster at the primary CA facility; and b) the requisite secret key shares or key components, needed to use and manage the disaster recovery cryptographic devices, are securely stored at an off-site location.		
	4) Backup copies of essential business information are regularly taken. The security requirements of these copies are consistent with the controls for the information backed up.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	5) The CA identifies and arranges for an alternate site where core PKI operations can be restored in the event of a disaster at the CA's primary site. Fall-back equipment and backup media are sited at a safe distance to avoid damage from disaster at the main site.		
	6) The CA's business continuity plans include 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.		
	7) The CA's business continuity plans address the recovery procedures used when computing resources, software, and/or data are corrupted or suspected to be corrupted.		
	8) Business continuity plans are tested regularly to ensure that they are up to date and effective.		
	9) Business continuity plans define an acceptable system outage time, recovery time, and the average time between failures as disclosed in the CP and/or CPS.		
	10) Business continuity plans are maintained by regular reviews and updates to ensure their continuing effectiveness.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	11) The CA maintains procedures for the termination, notification of affected entities, and for transferring relevant archived CA records to a custodian as disclosed in the CP and/or CPS.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	Monitoring and Compliance		
	Compliance with Legal Requirements		
3.9	WebTrust for CA Criteria - The CA maintains controls to provide reasonable assurance that: • it conforms with the relevant legal, regulatory and contractual requirements; • compliance with the CA's security policies and procedures is ensured; • the effectiveness of the system audit process is maximised and interference to and from the system audit process is minimised; and • unauthorised CA system usage is detected.		
	1) Relevant statutory, regulatory and contractual requirements are explicitly defined and documented.		
	2) The CA has implemented procedures to comply with legal restrictions on the use of		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	material in respect of intellectual property rights, and on the use of proprietary software products.		
	3) Controls are in place to ensure compliance with national agreements, laws, regulations or other instruments to control the access to or use of cryptographic hardware and software.		
	4) Procedures exist to ensure that personal information is protected in accordance with relevant legislation.		
	5) The information security policy addresses the following: a) the information that must be kept confidential by CA or RA; b) the information that is not considered confidential; c) the policy on release of information to law enforcement officials; d) information that can be revealed as part of civil discovery; e) the conditions upon which information may be disclosed with the subscriber's consent; and f) any other circumstances under which confidential information may be disclosed.		
	6) CA records are protected from loss, unauthorised destruction and falsification.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	7) Management authorises the use of information processing facilities and controls are applied to prevent the misuse of such facilities.		
	Review of Security Policy and Technical Compliance		
	8) Managers are responsible for ensuring that security procedures within their area of responsibility are carried out correctly.		
	9) The CA's operations are subject to regular review to ensure timely compliance with its CPS.		
	10) CA systems are periodically checked for compliance with security implementation standards.		
	System Audit Process		
	11) Audits of operational systems are planned and agreed such as to minimise the risk of disruptions to business processes.		
	12) Access to system audit tools is protected to prevent possible misuse or compromise.		
	Monitoring System Access and Use		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	13) Procedures for monitoring the use of CA systems are established which include the timely identification and follow up of unauthorised or suspicious activity. Alerting mechanisms are implemented to detect unauthorised access.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	Audit Logging		
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 • audit logs are reviewed periodically by authorised personnel.		
	Audit Logs		
	1) The CA generates automatic (electronic) and manual audit logs in accordance with the		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	requirements of the CP and/or CPS.		
	2) All journal entries include the following elements: a) date and time of the entry; b) serial or sequence number of entry (for automatic journal entries); c) kind of entry; c) source of entry (e.g., terminal, port, location, customer, etc.); and d) identity of the entity making the journal entry.		
	Events Logged		
	3) The CA logs the following CA and subscriber (if applicable) key life cycle management related events: a) CA key generation; b) installation of manual cryptographic keys and its outcome (with the identity of the operator); c) CA key backup; d) CA key storage; e) CA key recovery; f) CA key escrow activities (if applicable); g) CA key usage; h) CA key archival; i) withdrawal of keying material from service; j) CA key destruction; k) CA key transportation; l) CA key migration		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	m) identity of the entity authorising a key management operation; n) identity of the entities handling any keying material (such as key components or keys stored in portable devices or media); o) custody of keys and of devices or media holding keys; and p) compromise of a private key.		
	4) The CA logs the following cryptographic device life cycle management related events: a) device receipt and installation; b) placing into or removing a device from storage; c) device activation and usage; d) device de-installation; e) designation of a device for service and repair; and f) device retirement.		
	5) If the CA provides subscriber key management services, the CA logs the following subscriber key life cycle management related events: a) key generation; b) key distribution (if applicable); c) key backup (if applicable); d) key escrow (if applicable); e) key storage; f) key recovery (if applicable); g) key archival (if applicable); h) key destruction;		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	i) identity of the entity authorising a key management operation; and j) key compromise.		
	6) The CA records (or requires that the RA record) the following certificate application information: a) the method of identification applied and information used to meet subscriber requirements; b) record of unique identification data, numbers, or a combination thereof (e.g., applicants drivers license number) of identification documents, if applicable; c) storage location of copies of applications and identification documents; d) identity of entity accepting the application; e) method used to validate identification documents, if any; f) name of receiving CA or submitting RA, if applicable; g) the subscriber's acceptance of the Subscriber Agreement; and h) where required under privacy legislation, the Subscriber's consent to allow the CA to keep records containing personal data, pass this information to specified third parties,		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	and publication of certificates.		
	7) The CA logs the following certificate life cycle management related events: a) receipt of requests for certificate(s) – including initial certificate requests, renewal requests and rekey requests; b) submissions of public keys for certification; c) change of affiliation of an entity; d) generation of certificates; e) distribution of the CA's public key; f) certificate revocation requests; g) certificate revocation; h) certificate suspension requests (if applicable); i) certificate suspension and reactivation; and j) generation and issuance of Certificate Revocation Lists.		
	8) The CA logs the following security-sensitive events: a) security-sensitive files or records read or written including the audit log itself; b) actions taken against security-sensitive data; c) security profile changes; d) use of identification and authentication mechanisms, both successful and unsuccessful (including		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	multiple failed authentication attempts); e) system crashes, hardware failures and other anomalies; f) actions taken by individuals in Trusted Roles, computer operators, system administrators, and system security officers; g) change of affiliation of an entity; h) decisions to bypass encryption/authentication processes or procedures; and i) access to the CA system or any component thereof.		
	9) Audit logs do not record the private keys in any form (e.g., plaintext or enciphered).		
	10) CA computer system clocks are synchronised for accurate recording as defined in the CP and/or CPS that specifies the accepted time source.		
	Audit Log Protection		
	11) Current and archived audit logs are maintained in a form that prevents their modification, substitution, or unauthorised destruction.		
	12) Digital signatures are used to protect the integrity of audit logs where applicable or required to satisfy legal requirements.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	13) The private key used for signing audit logs is not used for any other purpose. This applies equally to a symmetric secret key used with a symmetric MAC mechanism.		
	Audit Log Archival		
	14) The CA archives audit log data on a periodic basis as disclosed in the CP and/or CPS.		
	15) In addition to possible regulatory stipulation, a risk assessment is performed to determine the appropriate length of time for retention of archived audit logs.		
	16) The CA maintains archived audit logs at a secure off-site location for a predetermined period as determined by risk assessment and legal requirements.		
	Review of Audit Logs		
	17) Current and archived audit logs are only retrieved by authorised individuals for valid business or security reasons.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	18) Audit logs are reviewed periodically according to the practices established in the CPS. The review of current and archived audit logs include a validation of the audit logs' integrity, and the timely identification and follow up of unauthorised or suspicious activity.		

Criteria related to CA Key Lifecycle Management Controls

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	CA Key Generation		
4.1	**WebTrust for CA Criteria -** The CA maintains controls to provide reasonable assurance that CA key pairs are generated in accordance with the CA's disclosed business practices and defined procedures specified within detailed key generation ceremony scripts. The CA's disclosed business practices include but are not limited to: a) generation of CA keys are undertaken in a physically secured environment (see §3.4); b) generation of CA keys are performed by personnel in trusted roles (see §3.3) under the principles of multiple person control and split knowledge; c) generation of CA keys occur within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's CPS; d) generation of CA keys are witnessed by an independent party and/or videotaped; and e) CA key generation activities are logged. The CA key generation script includes the following: a) definition of roles and participant responsibilities; b) approval for conduct of the key generation ceremony; c) cryptographic hardware and activation materials required for the ceremony;		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	d) specific steps performed during the key generation ceremony; e) physical security requirements for the ceremony location; f) procedures for secure storage of cryptographic hardware and activation materials following the key generation ceremony; g) sign-off from participants and witnesses indicating whether key generation ceremony was performed in accordance with the detailed key generation ceremony script; and notation of any deviations from the key generation ceremony script.		
	Generation of CA Keys Including Root CA Keys – General Requirements		
	1) Generation of CA keys occur within a cryptographic module meeting the applicable requirements of ISO 19790 and ISO 13491-1/FIPS 140-2 (or equivalent)/ANSI X9.66 and the business requirements in accordance with the CPS. Such cryptographic devices perform key generation using a random number generator (RNG) or pseudo random number generator (PRNG).		
	2) The CA generates its own key pair in the same cryptographic device in which it will be used or the key pair is injected directly from the device where it was generated into the device where it will be used.		
	3) CA key generation generates keys that:		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	a) use a key generation algorithm as disclosed within the CA's CP and/or CPS; b) have a key length that is appropriate for the algorithm and for the validity period of the CA certificate as disclosed in the CA's CP and/or CPS. The public key length to be certified by a CA is less than or equal to that of the CA's private signing key; and c) take into account requirements on parent and subordinate CA key sizes and have a key size in accordance with the CA's CP and/or CPS.		
	4) CA key generation ceremonies are independently witnessed by internal or external auditors.		
	5) Generation of CA keys shall be undertaken in a physically secured environment (see §3.4) by personnel in trusted roles (see §3.3) under the principles of multiple control and split knowledge.		
	Generation of CA Keys Including Root CA Keys – Script Requirements		
	6) The CA follows a CA key generation script for key generation ceremonies that includes the following: a) definition and assignment of participant roles and responsibilities; b) management approval for conduct of the key generation ceremony; c) specific cryptographic hardware, software and other materials		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	including identifying information, e.g., serial numbers; d) specific steps performed during the key generation ceremony, including; - Hardware preparation; - Verification of the integrity of the operating system and other software from its source (e.g. through the use of hash totals); - When a previously built master operating system image is being used, verification of the integrity of that image; - Operating system installation; - CA application installation and configuration; - CA key generation; - CA key backup; - CA certificate signing; - CA system shutdown; and - Preparation of materials for storage. e) physical security requirements for the ceremony location (e.g., barriers, access controls and logging controls); f) procedures for secure storage of cryptographic hardware and activation materials following the key generation ceremony (e.g., detailing the allocation of materials between storage locations); g) sign-off on the script or in a log from participants and witnesses indicating whether key generation ceremony was performed in accordance with the		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	detailed key generation ceremony script; and h) notation of any deviations from the key generation ceremony script (e.g., documentation of steps taken to address any technical issues).		
	7) The integrity of the hardware/software used for key generation and the interfaces to the hardware/software is tested before production usage.		
	CA Key Storage, Backup, and Recovery		
4.2	**WebTrust for CA Criteria -** The CA maintains controls to provide reasonable assurance that CA private keys remain confidential and maintain their integrity. The CA's private keys are backed up, stored and recovered by authorised personnel in trusted roles, using multiple person control in a physically secured environment.		
	1) The CA's private (signing and confidentiality) keys are stored and used within a secure cryptographic device meeting the appropriate ISO 15408 protection profile or FIPS 140-2 level requirement based on a risk assessment and the business requirements of the CA and in accordance with the CA's CPS and applicable Certificate Policy(s).		
	2) If the CA's private keys are not exported from a secure cryptographic module, then the CA private key is generated, stored and used within the same cryptographic module.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	3) If the CA's private keys are exported from a secure cryptographic module to secure storage for purposes of offline processing or backup and recovery, then they are exported within a secure key management scheme that may include any of the following: a) as cipher-text using a key which is appropriately secured; b) as encrypted key fragments using multiple control and split knowledge/ownership; or c) in another secure cryptographic module such as a key transportation device using multiple control.		
	4) Backup copies of the CA's private keys are subject to the same or greater level of security controls as keys currently in use. The recovery of the CA's keys is carried out in as secure a manner as the backup process, using multi-person control.		
	CA Public Key Distribution		
4.3	**WebTrust for CA Criteria -** The CA maintains controls to provide reasonable assurance that the integrity and authenticity of the CA public keys and any associated parameters are maintained during initial and subsequent distribution.		
	1) For the Root CA distribution process (e.g., using a self-signed certificate), an out-of-band notification mechanism is employed. Where a self-signed certificate is used for any CA, the CA provides a mechanism to verify the authenticity of the self-		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	signed certificate (e.g., publication of the certificate's fingerprint). For Intermediate, Issuing, and/or Subordinate CA public keys these are validated by using a chaining method or similar process to link back to the trusted Root Certificate.		
	2) The initial distribution mechanism for the CA's public key is controlled and initially distributed within a Certificate using one of the following methods: a) machine readable media (e.g., smart card, flash drive, CD ROM) from an authenticated source; b) embedding in an entity's cryptographic module; or c) other secure means that ensure authenticity and integrity.		
	3) The CA's public key is changed (rekeyed) periodically according to the requirements of the CPS with advance notice provided to avoid disruption of the CA services.		
	4) The subsequent distribution mechanism for the CA's public key is controlled in accordance with the CA's disclosed business practices.		
	5) If an entity already has an authenticated copy of the CA's public key, a new CA public key is distributed using one of the following methods: a) direct electronic transmission from the CA; b) placing into a remote cache or directory;		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	c) loading into a cryptographic module; or d) any of the methods used for initial distribution.		
	6) The CA provides a mechanism for validating the authenticity and integrity of the CA's public keys.		
	CA Key Usage		
4.4	**WebTrust For CA Criteria -** The CA maintains controls to provide reasonable assurance that CA keys are used only for their intended functions in their predetermined locations.		
	1) The activation of the CA private signing key is performed using multi-party control (i.e., m of n) with a minimum value of m (e.g., m greater than 2 for Root CAs).		
	2) If necessary, based on a risk assessment, the activation of the CA private key is performed using multi-factor authentication (e.g., smart card and password, biometric and password, etc.).		
	3) CA signing key(s) used for generating certificates and/or issuing revocation status information, are not used for any other purpose.		
	4) The CA ceases to use a key pair at the end of the key pair's defined operational lifetime or when the compromise of the private key is known or suspected.		
	5) An annual review is required by the PA on key lengths to determine the appropriate key usage period with recommendations acted upon.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	CA Key Archival		
4.5	**WebTrust for CA Criteria -** The CA maintains controls to provide reasonable assurance that archived CA keys remain confidential, secured, and are never put back into production.		
	1) Archived CA keys are subject to the same or greater level of security controls as keys currently in use.		
	2) All archived CA keys are destroyed at the end of the archive period using dual control in a physically secure site.		
	3) Archived keys are only accessed where historical evidence requires validation. Control processes are required to ensure the integrity of the CA systems and the key sets.		
	4) Archived keys are recovered for the shortest possible time period technically permissible to meet business requirements.		
	5) Archived keys are periodically verified to ensure that they are properly destroyed at the end of the archive period.		
	CA Key Destruction		
4.6	**WebTrust for CA Criteria -** The CA maintains controls to provide reasonable assurance that: • copies of CA keys that no longer serve a valid business purposes are destroyed in accordance with the CA's disclosed business practices; and		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	• copies of CA keys are completely destroyed at the end of the key pair life cycle in accordance with the CA's disclosed business practices.		
	1) The CA's private keys are not destroyed until the business purpose or application has ceased to have value or legal obligations have expired as disclosed within the CA's CPS.		
	2) Authorisation to destroy a CA private key and how the CA's private key is destroyed (e.g., token surrender, token destruction, or key overwrite) are limited in accordance with the CA's CPS.		
	3) All copies and fragments of the CA's private key are destroyed at the end of the key pair life cycle in a manner such that the private key cannot be retrieved.		
	4) If a secure cryptographic device is accessible and known to be permanently removed from service, all CA private keys stored within the device that have ever been or potentially could be used for any cryptographic purpose are destroyed.		
	5) If a CA cryptographic device is being permanently removed from service, then any key contained within the device that has been used for any cryptographic purpose is erased from the device.		
	6) If a CA cryptographic device case is intended to provide tamper-evident characteristics and the device is being		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	permanently removed from service, then the case is destroyed.		
	7) Backup or additional copies of CA keys that no longer serve a valid business purpose are destroyed in accordance with the CA's disclosed business practices.		
	8) The CA follows a CA key destruction script for key destruction ceremonies that includes the following: a) definition and assignment of participant roles and responsibilities; b) management approval for conduct of the key destruction ceremony; c) specific cryptographic hardware, software and other materials including identifying information, e.g., serial numbers, that contain the CA key copies to be destroyed; d) specific steps performed during the key destruction ceremony, including: i) HSM and/or cryptographic hardware zeroisation/initialisation ii) HSM and/or cryptographic hardware physical destruction iii) Deletion of any encrypted files containing the CA key or fragments thereof e) physical security requirements for the ceremony location (e.g., barriers, access controls and logging controls); f) procedures for secure storage of cryptographic hardware and any associated activation materials		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	following the key destruction ceremony pending their disposal or additional destruction g) sign-off on the script or in a log from participants and witnesses indicating whether the key destruction ceremony was performed in accordance with the detailed key destruction ceremony script; and h) notation of any deviations from the key destruction ceremony script (e.g., documentation of steps taken to address any technical issues).		
	9) CA key destruction ceremonies are independently witnessed by internal or external auditors.		
	CA Key Compromise		
4.7	**WebTrust for CA Criteria -** The CA maintains controls to provide reasonable assurance that continuity of operations is maintained in the event of the compromise of the CA's private keys and any certificates, signed with the compromised keys, are revoked and reissued.		
	1) The CA's business continuity plans address the compromise or suspected compromise of a CA's private keys as a disaster.		
	2) Disaster recovery procedures include the revocation and reissuance of all certificates that were signed with that CA's private key, in the event of the compromise or suspected compromise of a CA's private signing key.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	3) The recovery procedures used if the CA's private key is compromised include the following actions: a) how secure key usage in the environment is re-established; b) how the CA's old public key is revoked; c) how affected parties are notified (e.g., impacted CAs, Repositories, Subscribers and i) CVSPs); d) how the CA's new public key is provided to the end entities and Relying Parties together with the mechanism for their authentication; and e) how the subscriber's public keys are re-certified.		
	4) In the event that the CA has to replace its Root CA private key, procedures are in place for the secure and authenticated revocation of the following: a) the old CA root public key; b) the set of all certificates (including any self-signed) issued by a Root CA or any CA based on the compromised private key; and c) any subordinate CA public keys and corresponding certificates that require recertification.		
	5) The CA's business continuity plan for key compromise addresses who is notified and what actions are taken with system software and hardware, symmetric and asymmetric keys, previously generated signatures and encrypted data.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	CA Cryptographic Hardware Life Cycle Management		
4.8	**WebTrust for CA Criteria -** The CA maintains controls to provide reasonable assurance that: • devices used for private key storage and recovery, and the interfaces to these devices are tested before usage for integrity; • access to CA cryptographic hardware is limited to authorised personnel in trusted roles, using multiple person control; and • CA cryptographic hardware is functioning correctly.		
	1) CA cryptographic hardware which does not contain CA keys is sent from the manufacturer or alternate CA site via registered mail (or equivalent) using tamper evident packaging. Upon the receipt of CA cryptographic hardware from the manufacturer or alternate site, authorised CA personnel inspects the tamper evident packaging to determine whether the seal is intact.		
	2) Upon the receipt of CA cryptographic hardware from the manufacturer, acceptance testing and verification of firmware settings is performed. Upon the receipt of CA cryptographic hardware that has been serviced or repaired, acceptance testing and verification of firmware settings is performed.		
	3) To prevent tampering, CA cryptographic hardware is stored and used in a secure site, with access		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	limited to authorised personnel, having the following characteristics: a) inventory control processes and procedures to manage the origination, arrival, condition, departure and destination of each device; b) access control processes and procedures to limit physical access to authorised personnel; c) recording of all successful or failed access attempts to the CA facility and device storage mechanism (e.g., a safe) in audit logs; d) incident handling processes and procedures to handle abnormal events, security breaches, and investigation and reports; and e) monitoring processes and procedures to verify the ongoing effectiveness of the controls.		
	4) When not attached to the CA system, the CA cryptographic hardware is stored in a tamper resistant container that is stored securely under multiple controls (i.e., a safe).		
	5) The handling of CA cryptographic hardware, including the following tasks, is performed in the presence of no less than two trusted employees: a) installation of CA cryptographic hardware; b) removal of CA cryptographic hardware from production; c) servicing or repair of CA cryptographic hardware (including installation of new hardware, firmware, or software); and		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	d) disassembly and permanent removal from use.		
	6) Devices used for private key storage and recovery and the interfaces to these devices are tested before usage for integrity.		
	7) Correct processing of CA cryptographic hardware is verified on a periodic basis.		
	8) Diagnostic support is provided during troubleshooting of CA cryptographic hardware in the presence of no less than two trusted employees.		
	CA Key Escrow (if applicable)		
4.9	**WebTrust for CA Criteria -** The CA maintains controls to provide reasonable assurance that escrowed CA private signing keys remain confidential.		
	1) If a third party provides CA private key escrow services, a contract exists that outlines the liabilities and remedies between the parties.		
	2) If CA private signing keys are held in escrow, escrowed copies of the CA private signing keys have the same or greater level of security controls as keys currently in use.		
	CA Key Transportation (if applicable)		
4-10	**WebTrust for CA Criteria -** The CA maintains controls to provide reasonable assurance that: • CA private keys that are physically transported from one		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	facility to another remain confidential and maintain their integrity; • CA hardware containing CA private keys, and associated activation materials, are prepared for transport in a physically secure environment (see §3.4) by authorised personnel in trusted roles, using multiple person controls, and are transported within sealed tamper evident packaging; • CA keys and associated activation materials are transported in a manner that prevents the key from being activated or accessed during the transportation event; and • CA key transportation events are logged.		
	1) CA keys are prepared for transport in a physically secure environment (see §3.4) by personnel in Trusted Roles and under multi-person control.		
	2) CA keys remain in a physically secure environment (see §3.4) until ready to be transported by CA personnel or common carrier.		
	3) CA keys are only transported on hardware devices and in tamper-evident packaging as disclosed in the CA's business practices.		
	4) If the hardware device contains the entire CA key, it is physically transported by at least two CA employees and remains under multi-person control from origin to destination.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	5) If the CA key is divided into fragments on multiple hardware devices: a) If transported by CA employees, each fragment is transported separately using different transportation routes, methods, and/or times; or b) If transported by common carrier, each fragment is sent using a different common carrier at different times. Shipments require signature service, tracking, are insured.		
	6) Activation materials are transported separately from the CA key (i.e. by a different method and/or at a different time) in tamper-evident packaging.		
	7) Upon receipt at the destination, packaging for CA keys and activation materials are reviewed for evidence of tampering. If evidence of tampering is discovered, the Policy Authority is notified of a possible breach event.		
	8) Upon receipt at the destination, CA keys and activation materials are stored in a physically secure environment (see §3.4) by personnel in Trusted Roles and under multi-person control.		
	9) Personnel involved in a CA key transportation event are in Trusted Roles and have received training in their role and responsibilities.		
	10) A log is maintained of all actions taken as part of the CA key transportation event and is retained in		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	accordance with the CA's disclosed business practices.		
	11) Internal or external auditors accompany CA personnel during CA key transportation events.		
	CA Key Migration (if applicable)		
4.11	WebTrust for CA Criteria - The CA maintains controls to provide reasonable assurance that: • CA keys migrated from one secure cryptographic device to another, other than for the purposes of routine backup and restoration (see §4.2), are completed in a physically secure environment (see §3.4) by those in Trusted Roles under multi-person control; • hardware and software tools used during the CA key migration process are tested by the CA prior to the migration event; and • CA key migration events follow a documented script and are logged.		
	1) CA key migration events occur in a physically secure environment (see §3.4) by those in Trusted Roles under multi-person control.		
	2) Vendor-supplied hardware and software tools are tested by the CA prior the key migration event, and are operated in accordance with vendor-supplied documentation and instructions.		
	3) In-house developed software tools are developed and tested by the CA prior to the key migration event in		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	accordance with its standard software development process (see §3.7).		
	4) The CA follows a CA key migration script for key migration events that includes the following: a) definition and assignment of participant roles and responsibilities; b) management approval for conduct of the key migration event c) specific cryptographic hardware, software and other materials including identifying information, e.g., serial numbers, that contain the CA key copies to be migrated and new hardware where the keys are being migrated to; d) specific steps performed during the key migration ceremony, including; i) Hardware preparation ii) Software tool installation and setup iii) Cryptographic hardware setup and initialisation iv) CA key migration v) CA key verification e) physical security requirements for the event location (e.g., barriers, access controls and logging controls); f) procedures for secure storage of cryptographic hardware and any associated activation materials following the migration event g) sign-off on the script or in a log from participants and witnesses indicating whether the key		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	migration was performed in accordance with the detailed key migration script; and h) notation of any deviations from the key migration script (e.g., documentation of steps taken to address any technical issues).		
	5) A log is maintained of all actions taken as part of the CA key migration event and is retained in accordance with the CA's disclosed business practices.		
	6) CA key migration events are witnessed by internal or external auditors.		
	7) Upon successful completion of a CA key migration event, remaining copies of the CA keys, and older cryptographic hardware that no longer serve a business purpose are securely destroyed in accordance with the CA's disclosed business practices (see §4.5).		

Criteria related to Subscriber Key Lifecycle Controls

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	CA-Provided Subscriber Key Generation Services (if supported)		
5.1	**WebTrust for CA Criteria -** The CA maintains controls to provide reasonable assurance that: • subscriber keys generated by the CA (or RA or card bureau) are generated within a secure cryptographic device based on a risk assessment and the		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	business requirements of the CA in accordance with the CA's disclosed business practices; and • subscriber keys generated by the CA (or RA or card bureau) are securely distributed to the subscriber by the CA (or RA or card bureau) in accordance with the CA's disclosed business practices.		
	CA (or RA or Card Bureau) Provided Subscriber Key Generation		
5.1.1	Subscriber key generation is performed within a secure cryptographic device meeting the applicable ISO 15782-1/FIPS 140-2/ANSI x9.66 requirements based on a risk assessment and the business requirements of the CA and in accordance with the applicable CP. Such cryptographic devices perform subscriber key generation using a random number generator (RNG) or pseudo random number generator (PRNG) as specified in the ANSI X9 or ISO standard ISO/IEC 18032.		
5.1.2	Subscriber key generation performed by the CA (or RA or card bureau) uses a key generation algorithm as specified in the CP.		
5.1.3	Subscriber key generation performed by the CA (or RA) uses a prime number generator as specified in an ANSI X9 or ISO standard.		
5.1.4	Subscriber key generation performed by the CA (or RA or card bureau) results in key sizes in accordance with the CP.		
5.1.5	Subscriber key generation performed by the CA (or RA) is performed by authorised personnel in accordance with the CA's CPS.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
5.1.6	When subscriber key generation is performed by the CA (or RA or card bureau), the CA (or RA or card bureau) securely (confidentially) delivers the subscriber key pair(s) generated by the CA (or RA or card bureau) to the subscriber in accordance with the CP.		
	CA-Provided Subscriber Key Generation Services (if supported)		
5.2	**WebTrust for CA Criteria -** The CA maintains controls to provide reasonable assurance that: • subscriber private keys stored by the CA remain confidential and maintain their integrity; • subscriber private keys archived and escrowed by the CA remain confidential; and • subscriber private keys stored by the CA are completely destroyed at the end of the key pair life cycle.		
	CA-Provided Subscriber Key Storage, Backup and Recovery		
5.2.1	Subscriber private keys stored by the CA (or RA) are stored in encrypted form using a cryptographic algorithm and key length based on a risk assessment and requirements of the CP.		
5.2.2	If the CA generates key pair(s) on behalf of a Subscriber, the CA (or RA) ensures that the subscriber's private keys are not disclosed to any entity other than the owner (i.e., the subscriber) of the keys.		
5.2.3	If the CA (or RA) generates public/private signing key pair(s), it does not maintain a copy of any private signing key, once the subscriber confirms receipt of that key.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
5.2.4	If the CA (or RA) provides subscriber (confidentiality) key storage, backup and recovery, subscriber private (confidentiality) key backup and recovery services are only performed by authorised personnel.		
5.2.5	If the CA (or RA) provides subscriber key storage, backup and recovery, controls exist to ensure that the integrity of the subscriber's private (confidentiality) key is maintained throughout its life cycle.		
	CA-Provided Subscriber Key Archival		
5.2.6	Subscriber private (confidentiality) keys archived by the CA are stored in encrypted form using a cryptographic algorithm and key length based on a risk assessment and the requirements of the CP.		
5.2.7	If the CA provides subscriber (confidentiality) key archival, all archived Subscriber keys are destroyed at the end of the archive period.		
	CA-Provided Subscriber Key Destruction		
5.2.8	If the CA provides subscriber (confidentiality) key storage, authorisation to destroy a subscriber's private key and the means to destroy the subscriber's private (confidentiality) key (e.g., key overwrite) is limited in accordance with the CP.		
5.2.9	If the CA provides subscriber (confidentiality) key storage, all copies and fragments of the subscriber's private key are destroyed at the end of the key pair life cycle.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	CA-Provided Subscriber Key Escrow		
5.2.10	Subscriber private (confidentiality) keys escrowed by the CA are stored in encrypted form using a cryptographic algorithm and key length based on a risk assessment and the requirements of the CP.		
	Integrated Circuit Card (ICC) Lifecycle Management (if supported)		
5.3	**WebTrust for CA Criteria -** The CA maintains controls to provide reasonable assurance that: • ICC procurement, preparation and personalisation are securely controlled by the CA (or RA or card bureau); • ICC Application Data File (ADF) preparation is securely controlled by the CA (or RA); • ICC usage is enabled by the CA (or RA or card bureau) prior to ICC issuance; • ICC deactivation and reactivation are securely controlled by the CA (or RA); • ICCs are securely stored and distributed by the CA (or RA or card bureau); • ICCs are securely replaced by the CA (or RA or card bureau); and • ICCs returned to the CA (or RA or card bureau) are securely terminated.		
	ICC Procurement		
5.3.1	If the CA or RA engages a card bureau then a formal contract exists between the relevant parties. While card issuing		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	functions may be delegated to third parties the CA retains responsibility and liability for the ICCs.		
5.3.2	ICCs are logically protected during transport between the card manufacturer and the card issuer through the use of a secret transport key or pass phrase.		
5.3.3	ICCs issued to subscribers meet the appropriate ISO 15408 protection profile, ISO card standard (e.g., ISO 7810, 7811 parts 1-5, 7813, 7816, 10202) or FIPS 140-2 level requirement based on a risk assessment and the requirements of the CP.		
5.3.4	The card bureau verifies the physical integrity of ICCs upon receipt from the card manufacturer.		
5.3.5	ICCs are securely stored and under inventory control while under the control of the card issuer.		
	Card Preparation and Personalisation		
5.3.6	The CA (or RA), as the card issuer, controls ICC personalisation (the loading of Common Data File (CDF) data and its related cryptographic keys).		
5.3.7	Common data that identify the ICC, the card issuer, and the cardholder are stored by the card issuer in the ICC Common Data File (CDF). Common Data File (CDF) activation is performed by the CA (or RA), as the card issuer, using a securely controlled process.		
5.3.8	ICC preparation processes and procedures, including the following, exist and are followed: a) loading of the card operating system; b) creation of logical data structures (card file system and card security domains);		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	c) loading of applications; and d) logically protecting the ICC to prevent unauthorised modification of the card operating system, card file system, card security domains, and applications.		
5.3.9	ICC personalisation processes and procedures, including the following, exist and are followed: a) the loading of identifying information onto the card; b) generation of subscriber key pair(s) in accordance with the CP; c) loading subscriber private key(s) onto the ICC (if generated outside the card) in encrypted form; d) loading subscriber Certificate(s) onto the ICC; e) loading the CA and other Certificates for the contractual environment onto the ICC; and f) logically protecting the ICC from unauthorised access.		
5.3.10	The card bureau or CA (or RA) logs ICC preparation and personalisation in an audit log.		
5.3.11	An ICC is not issued unless the card has been prepared and personalised by the card bureau, the CA or the RA.		
5.3.12	An ICC is unusable unless in an activated or reactivated state.		
	ICC Storage and Distribution		
5.3.13	ICCs are securely stored prior to distribution.		
5.3.14	Processes and procedures exist and are followed for the distribution, tracking		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	and accounting for the safe receipt of Subscriber ICCs to subscribers.		
5.3.15	ICC initial activation data (initialising PIN) is securely communicated to the subscriber or where applicable the Subscriber using an out-of-band method. The subscriber is encouraged to change the initial activation data upon receipt to make the card active.		
5.3.16	ICC distribution is logged by the card bureau or CA (or RA) in an audit log.		
	Subscriber ICC Usage		
5.3.17	The subscriber is provided with a mechanism that protects the access to the card data including the private keys stored on the ICC during use by the Subscriber (i.e., PIN access control mechanism Cardholder Verification Method).		
5.3.18	The subscriber private keys on the ICC are not exported to an application to undertake cryptographic (i.e., signing) functions.		
5.3.19	The subscriber is required to use a mutual authentication mechanism for cryptographic application and card functions to ensure system integrity.		
5.3.20	The subscriber is required to use an application that displays the message or the message's digest to the subscriber prior to signing message (or transaction) data. The subscriber ICC application produces audit logs of all uses of the ICC. This also includes all attempts in the private key owner verification process.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
5.3.21	The ICC is used by the subscriber or where applicable the Subscriber in accordance within the terms of the CP.		
	ICC Deactivation and Reactivation		
5.3.22	Application Data File (ADF) deactivation can be performed only by the CA, as the application supplier.		
5.3.23	Common Data File (CDF) deactivation can be performed only by the CA, as the card issuer.		
5.3.24	CDF reactivation is conducted under the control of the CA, as the card issuer.		
5.3.25	ADF reactivation is conducted under the control of the CA, as the application supplier.		
5.3.26	ADF deactivation, CDF deactivation, CDF reactivation, and ADF reactivation are logged.		
	ICC Replacement		
5.3.27	Processes and procedures exist and are followed for replacement of a subscriber's lost or damaged ICC.		
5.3.28	In the event of card loss or damage, subscriber certificates are renewed or rekeyed in accordance with the CP (see clauses **Error! Reference source not found.** and **Error! Reference source not found.**).		
5.3.29	ICC replacement is logged by the card bureau or CA (or RA) in an audit log.		
	ICC Termination		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
5.3.30	All ICCs returned to the ICC or CA (or RA) are deactivated or securely destroyed to prevent unauthorised use.		
5.3.31	Common Data File (CDF) termination is controlled by the CA, as the card issuer.		
5.3.32	ICC termination is logged by the card bureau or CA (or RA) in an audit log.		
5.4	Requirements for Subscriber Key Management		
	WebTrust for CA Criteria - The CA maintains controls to provide reasonable assurance that: • requirements for protection of subscriber keys are communicated to subscribers; and • any subscriber key management tools provided by the CA support the requirements of the CA's business practices disclosure.		
	Subscriber Key Generation		
5.4.1	The CP specifies the appropriate ISO 19790/FIPS 140-2 level requirement for cryptographic modules used for subscriber key generation.		
5.4.2	The CP specifies the key generation algorithm(s) that is used for subscriber key generation.		
5.4.3	The CP specifies the acceptable key sizes for subscriber key generation.		
	Subscriber Key Storage, Backup and Recovery		
5.4.4	The CA or RA provides or makes available the mechanisms to allow the Subscriber to access (i.e., private key		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	owner verification method), manage and control the usage of their private keys.		
5.4.5	The CP specifies the private key protection requirements for stored subscriber private keys.		
5.4.6	The CP states the circumstances and authority of when the subscriber's private key will be restored and the control processes.		
5.4.7	The CP specifies the private key protection requirements for backup copies of subscriber private keys stored by the subscriber.		
	Subscriber Key Usage		
5.4.8	Subscriber Agreements describe the required processes to be followed by the Subscriber of any use of the cryptographic mechanism (e.g., HSM or ICC and software application).		
5.4.9	The CP specifies the acceptable uses for subscriber key pairs.		
5.4.10	The CP specifies the requirements for subscriber key usage.		
	Subscriber Key Archival		
5.4.11	The CP specifies the private key protection requirements for archived subscriber private keys.		
5.4.12	The CP specifies the requirements for destruction of archived subscriber keys at the end of the archive period.		
	Subscriber Key Destruction		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
5.4.13	The CP specifies the means through which subscriber key destruction is performed.		
5.4.14	The CP or CPS specifies the requirements for destruction of all copies and fragments of the subscriber's private key at the end of the key pair life cycle.		
	Subscriber Cryptographic Hardware Life Cycle Management		
5.4.15	If required, the CP specifies the requirements for use and handling of cryptographic hardware and subscriber authentication processes (and subsequent actions) where the cryptographic hardware is in other physical locations (i.e., an HSM attached to a mainframe or remote server).		
	Subscriber Key Compromise		
5.4.16	The CP specifies the requirements for notification of the CA or RA in the event of subscriber key compromise.		

Criteria related to Certificate Lifecycle Management

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	Subscriber Registration		
6.1	**WebTrust for CA Criteria -** The CA maintains controls to provide reasonable assurance that: For authenticated certificates		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	• subscribers are accurately identified in accordance with the CA's disclosed business practices; • subscribers' domain names and IP addresses are accurately validated in accordance with the CA's disclosed business practices; and • subscribers' certificate requests are accurate, authorised and complete. For domain validated certificates • Subscribers' domain names are accurately validated in accordance with the CA's disclosed business practices; and • Subscriber's certificate requests are accurate and complete.		
	Identification and Authentication		
6.1.1	For authenticated certificates, the CA verifies or requires that the RA verify the credentials presented by a subscriber as evidence of identity or authority to perform a specific role in accordance with the requirements of the CP. a) For individual end entity certificates, the CA or RA verifies the identity of the person whose name is to be included in the subscriber distinguished name field of the certificate. An unauthenticated individual name is not included in the subscriber distinguished name. b) For organisational certificates (including role based, server, network resource, code signing, etc.), the CA or RA verifies the legal existence of the organisation's name and the authority of the requesting party to be included in the		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	organisation attribute in the subscriber distinguished name field of the certificate. An unauthenticated organisation name is not included in a certificate. c) For organisational certificates containing a domain name of an organisation, the CA or RA verifies the organisation's ownership, control, or right to use the domain name and the authority of the requesting party included in the common name attribute of the subscriber distinguished name field of the certificate. An unauthenticated domain name is not included in a certificate.		
6.1.2	For domain and/or IP address validated certificates, the CA validates or requires that the RA validate (as determined by the CP) the organisation's ownership, control, or right to use the domain name and/or IP address.		
6.1.3	The CA or RA verifies the accuracy of the information included in the requesting entity's certificate request in accordance with the CP.		
6.1.4	The CA or RA checks the Certificate Request for errors or omissions in accordance with the CP.		
6.1.5	For end entity certificates, the CA uses the RA's public key contained in the requesting entity's Certificate Request to verify signature on the Certificate Request submission.		
6.1.6	The CA verifies the uniqueness of the subscriber's distinguished name within the boundaries or community defined by the CP.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
6.1.7	Encryption and access controls are used to protect the confidentiality and integrity of registration data in transit and in storage.		
6.1.8	At the point of registration (before certificate issuance) the RA or CA informs the Subscriber of the terms and conditions regarding use of the certificate.		
6.1.9	Before certificate issuance, the CA informs the Subscriber of the terms and conditions regarding use of the certificate.		
	Certificate Request		
6.1.10	The CA requires that an entity requesting a certificate must prepare and submit the appropriate certificate request data (Registration Request) to an RA (or the CA) as specified in the CP.		
6.1.11	The CA requires that the requesting entity submit its public key in a self-signed message to the CA for certification. The CA requires that the requesting entity digitally sign the Registration Request using the private key that relates to the public key contained in the Registration Request in order to: a) allow the detection of errors in the certificate application process; and b) prove possession of the companion private key for the public key being registered.		
6.1.12	The certificate request is treated as acceptance of the terms of conditions by the requesting entity to use that certificate as described in the Subscriber Agreement.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
6.1.13	The CA validates the identity of the RA authorised to issue registration requests under a specific CP.		
6.1.14	The CA requires that RAs submit the requesting entity's certificate request data to the CA in a message (Certificate Request) signed by the RA. The CA verifies the RA's signature on the Certificate Request.		
6.1.15	The CA requires that the RA secure that part of the certificate application process for which it (the RA) assumes responsibility in accordance with the CA's CPS.		
6.1.16	The CA requires that RAs record their actions in an audit log.		
6.1.17	The CA verifies the authenticity of the submission by the RA in accordance with the CA's CPS.		
6.2	Certificate Renewal (if supported)		
	WebTrust for CA Criteria - The CA maintains controls to provide reasonable assurance that certificate renewal requests are accurate, authorised and complete.		
	Certificate Renewal Request		
6.2.1	The Certificate Renewal Request includes at least the subscriber's Distinguished Name, the Serial Number of the certificate (or other information th0 at identifies the certificate), and the requested validity period. (The CA will only renew certificates that were issued by itself.)		
6.2.2	The CA requires that the requesting entity digitally sign the Certificate		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	Renewal Request using the private key that relates to the public key contained in the requesting entity's existing public key certificate.		
6.2.3	The CA issues a new certificate using the subscriber's previously certified public key, only if its cryptographic security is still sufficient for the new certificate's intended lifetime and no indications exist that the subscriber's private key has been compromised.		
6.2.4	For renewal of authenticated certificates, the CA or the RA process the certificate renewal data to verify the identity of the requesting entity and to identify the certificate to be renewed.		
6.2.5	For domain validated certificates, the CA or the RA process the certificate renewal data to re-validate the domain in accordance with the requirements of the CP.		
6.2.6	The CA or the RA validate the signature on the Certificate Renewal Request.		
6.2.7	The CA verifies the existence and validity of the certificate to be renewed. The CA does not renew certificates that have been revoked, expired or suspended.		
6.2.8	The CA or the RA verifies that the request, including the extension of the validity period, meets the requirements defined in the CP.		
6.2.9	The CA requires that RAs submit the Certificate Renewal Data to the CA in a message (Certificate Renewal Request) signed by the RA.		
6.2.10	The CA requires that the RA secures that part of the certificate renewal process for which it (the RA) assumes		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	responsibility in accordance with the CP.		
6.2.11	The CA requires that RAs record their actions in an audit log.		
6.2.12	The CA verifies the authenticity of the submission by the RA.		
6.2.13	The CA verifies the RA's signature on the Certificate Renewal Request.		
6.2.14	The CA checks the Certificate Renewal Request for errors or omissions. This function may be delegated explicitly to the RA.		
6.2.15	The CA or RA notifies Subscribers prior to the expiration of their certificate of the need for renewal in accordance with the CP.		
6.2.16	The CA issues a signed notification indicating the certificate renewal has been successful.		
6.2.17	The CA makes the new certificate available to the end entity in accordance with the CP.		
6.3	Certificate Rekey		
	WebTrust for CA Criteria - The CA maintains controls to provide reasonable assurance that certificate rekey requests, including requests following certificate revocation or expiration, are accurate, authorised and complete.		
6.3.1	A Certificate Rekey Request includes at least the subscriber's distinguished name, the serial number of the certificate, and the requested validity period to allow the CA or the RA to identify the certificate to rekey.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
6.3.2	The CA requires that the requesting entity digitally sign, using the existing private key, the Certificate Rekey Request containing the new public key.		
6.3.3	For authenticated certificates, the CA or the RA processes the Certificate Rekey Request to verify the identity of the requesting entity and identify the certificate to be rekeyed.		
6.3.4	For domain validated certificates, the CA or the RA process the Certificate Rekey Request to re-validate the domain in accordance with the requirements of the CP.		
6.3.5	The CA or the RA validates the signature on the Certificate Rekey Request.		
6.3.6	The CA or the RA verifies the existence and validity of the certificate to be rekeyed.		
6.3.7	The CA or the RA verifies that the Certificate Rekey Request meets the requirements defined in the relevant CP.		
6.3.8	If an external RA is used, the CA requires that RAs submit the entity's certificate rekey request to the CA in a message signed by the RA.		
6.3.9	If an external RA is used, the CA requires that the RA secure that part of the certificate rekey process for which it (the RA) assumes responsibility.		
6.3.10	If an external RA is used, the CA requires that external RAs record their actions in an audit log.		
6.3.11	If an external RA is used, the CA verifies the RA's signature on the Certificate Rekey Request.		
6.3.12	The CA or the RA checks the Certificate Rekey Request for errors or omissions.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
6.3.13	The CA or RA notifies Subscribers prior to the expiration of their certificate of the need for rekey.		
6.3.14	Prior to the generation and issuance of rekeyed certificates, the CA or RA verifies the following: a) the signature on the certificate rekey data submission; b) the existence and validity supporting the rekey request; and c) that the request meets the requirements defined in the CP.		
6.4	Certificate Issuance		
	WebTrust for CA Criteria - The CA maintains controls to provide reasonable assurance that certificates are generated and issued in accordance with the CA's disclosed business practices.		
6.4.1	The CA generates certificates using Certificate Request Data and manufactures the certificate as defined by the appropriate Certificate Profile in accordance with ISO 9594/X.509 and ISO 15782-1 formatting rules as disclosed within the CP.		
6.4.2	Validity periods are set in the CP and are formatted in accordance with ISO 9594/X.509 and ISO 15782-1 as disclosed within the CP.		
6.4.3	Extension fields are formatted in accordance with ISO 9594/X.509 and ISO 15782-1 as disclosed within the CP.		
6.4.4	The CA signs the end entity's public key and other relevant information with the CA's private signing key.		
6.4.5	The CA publishes the certificate after the certificate has been accepted by the requesting entity as disclosed in the CA's business practices.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
6.4.6	When an RA is used, the CA notifies the RA when a certificate is issued to a subscriber for whom the RA submitted a certificate request.		
6.4.7	Certificates are issued based on approved subscriber registration, certificate renewal or certificate rekey requests in accordance with the CP.		
6.4.8	The CA issues a signed notification to the RA when a certificate is issued to a subscriber for whom the RA submitted a certificate request.		
6.4.9	The CA issues an out-of-band notification to the Subscriber when a certificate is issued. Where this notification includes initial activation data, then control processes ensure safe delivery to the Subscriber.		
6.4.10	Whether certificates expire, are revoked or are suspended, copies of certificates are retained for the appropriate period of time specified in the CP.		
6.5	Certificate Distribution		
6.5.1	**WebTrust for CA Criteria -** The CA makes the certificates issued by the CA available to relevant parties using an established mechanism (e.g., a repository such as a directory) in accordance with the CP.		
6.5.2	Only authorised CA personnel administer the CA's repository or alternative distribution mechanism.		
6.5.3	The performance of the CA's repository or alternative distribution mechanism is monitored and managed.		
6.5.4	The integrity of the repository or alternative distribution mechanism is maintained and administered.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
6.5.5	Where required under privacy legislation, certificates are made available for retrieval only in those cases for which the subscriber's consent is obtained.		
6.6	Certificate Revocation		
	WebTrust for CA Criteria - The CA maintains controls to provide reasonable assurance that certificates are revoked, based on authorised and validated certificate revocation requests within the time frame in accordance with the CA's disclosed business practices.		
6.6.1	The CA provides a means of rapid communication to facilitate the secure and authenticated revocation of the following: a) one or more certificates of one or more subscribers; b) the set of all certificates issued by a CA based on a single public/private key pair used by a CA to generate certificates; and c) all certificates issued by a CA, regardless of the public/private key pair used.		
6.6.2	The CA verifies or requires that the RA verify the identity and authority of the entity requesting revocation of a certificate in accordance with the CP.		
6.6.3	If an external RA accepts revocation requests, the CA requires that the RA submit signed certificate revocation requests to the CA in an authenticated manner in accordance with the CP.		
6.6.4	If an external RA accepts and forwards revocation requests to the CA, the CA provides a signed acknowledgement of		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	the revocation request and confirmation of actions to the requesting RA.		
6.6.5	The CA updates the Certificate Revocation List (CRL) and other certificate status mechanisms in the timeframes specified within the CP and in accordance with the format defined in ISO 9594/X.509 and ISO 15782-1.		
6.6.6	The CA records all certificate revocation requests and their outcome in an audit log.		
6.6.7	The CA or RA may provide an authenticated acknowledgement (signature or similar) of the revocation to the entity who perpetrated the revocation request.		
6.6.8	Where certificate renewal is supported, when a certificate is revoked, all valid instances of the certificate are also revoked and are not reinstated.		
6.6.9	The Subscriber of a revoked or suspended certificate is informed of the change of status of its certificate.		
6.7	Certificate Suspension (if supported)		
	WebTrust for CA Criteria - The CA maintains controls to provide reasonable assurance that certificates are suspended based on authorised and validated certificate suspension requests within the time frame in accordance with the CA's disclosed business practices.		
6.7.1	The CA provides a means of rapid communication to facilitate the secure and authenticated suspension of the following: a) one or more certificates of one or more subscribers;		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	b) the set of all certificates issued by a CA based on a single public/private key pair used by a CA to generate certificates; and c) all certificates issued by a CA, regardless of the public/private key pair used.		
6.7.2	The CA verifies or requires that the external RA verify the identity and authority of the entity requesting suspension and reactivation of a certificate in accordance with the CP.		
6.7.3	If an external RA accepts suspension requests, the RA submits signed certificate suspension requests to the CA in an authenticated manner in accordance with the CP.		
6.7.4	The CA or RA notifies the Subscriber in the event of a certificate suspension.		
6.7.5	Certificate suspension requests are processed and validated in accordance with the requirements of the CP.		
6.7.6	The CA updates the Certificate Revocation List (CRL) and other certificate status mechanisms upon certificate suspension. Changes in certificate status are completed in a time frame determined by the CP.		
6.7.7	Certificates are suspended only for the allowable length of time in accordance with the CP.		
6.7.8	Once a certificate suspension (hold) has been issued, the suspension is handled in one of the following three ways: a) an entry for the suspended certificate remains on the CRL with no further action; b) the CRL entry for the suspended certificate is replaced by a revocation entry for the same certificate; or		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	c) the suspended certificate is explicitly released and the entry removed from the CRL.		
6.7.9	A certificate suspension (hold) entry remains on the CRL until the expiration of the underlying certificate or the expiration of the suspension, whichever is first.		
6.7.10	The CA updates the Certificate Revocation List (CRL) and other certificate status mechanisms upon the lifting of a certificate suspension in accordance with the CA's CP.		
6.7.11	The CA verifies or requires that the external RA verify the identity and authority of the entity requesting that the suspension of a certificate be lifted.		
6.7.12	Certificate suspensions and the lifting of certificate suspensions are recorded in an audit log.		
6.8	Certificate Validation		
	WebTrust for CA Criteria - The CA maintains controls to provide reasonable assurance that timely, complete and accurate certificate status information (including Certificate Revocation Lists and other certificate status mechanisms) is made available to relevant entities (Subscribers and Relying Parties or their agents) in accordance with the CA's disclosed business practices.		
6.8.1	The CA makes certificate status information available to relevant entities (Relying Parties or their agents) using an established mechanism in accordance with the CP. This is achieved using: a) Request Response Method – A request signed by the Relying Party to the Certificate Status Provider's		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	responder. In turn, the Certificate Status Provider's responder responds with the certificate status duly signed. (OCSP is an example protocol using this method.) b) Delivery Method – A CRL signed by the CA and published within the policy's time frame.		
	Certificate Revocation List (CRL) Controls		
6.8.2	The CA digitally signs each CRL that it issues so that entities can validate the integrity of the CRL and the date and time of issuance.		
6.8.3	The CA issues CRLs at regular intervals, as specified in the CP, even if no changes have occurred since the last issuance.		
6.8.4	At a minimum, a CRL entry identifying a revoked certificate remains on the CRL until the end of the certificate's validity period.		
6.8.5	If certificate suspension is supported, a certificate suspension (hold) entry, with its original action date and expiration date remain on the CRL until the normal expiration of the certificate or until the suspension is lifted.		
6.8.6	CRLs are archived in accordance with the requirements of the CP including the method of retrieval.		
6.8.7	CAs include a monotonically increasing sequence number for each CRL issued by that CA.		
6.8.8	The CRL contains entries for all revoked unexpired certificates issued by the CA.		
6.8.9	Old CRLs are retained for the appropriate period of time specified in the CA's CP.		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
6.8.10	Whether certificates expire, are revoked or are suspended, copies of certificates are retained for the appropriate period of time as disclosed in the CP.		
	Online Certificate Status Protocol (OCSP) (or other online status mechanism) Controls		
6.8.11	If an online certificate status collection method (e.g., OCSP) is used, the CA requires that certificate status inquiries (e.g., OCSP requests) contain all required data in accordance with the CP.		
6.8.12	Upon the receipt of a certificate status request (e.g., an OCSP request) from a Relying Party or its agent, the CA returns a definitive response to the Relying Party or its agent if: a) the request message is well formed; b) the Certificate Status Provider responder is configured to provide the requested service; c) the request contains the information (i.e., certificate identity – Serial number, OID, etc.) needed by the Certificate Status Provider responder in accordance with the CP; and d) the Certificate Status Provider's responder is able to locate the certificate and interpret its status. Where these conditions are met, the CA or Certificate Status Provider produces a signed response message indicating the certificate's status in accordance with the CP. If any of the above conditions are not met then a status of unknown may be returned.		
6.8.13	All response messages are digitally signed and include all required data in accordance with the CP.		

Criteria related to Subordinate CA and Cross Certificate Lifecycle Management Controls

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	Subordinate CA Certificate and Cross Certificate Lifecycle Management		
7.1	**WebTrust for CA Criteria -** The CA maintains controls to provide reasonable assurance that: • subordinate CA and cross certificate requests are accurate, authenticated and approved; • subordinate CA and cross certificate replacement (renewal and rekey) requests are accurate, authorised, complete; • new, renewed and rekeyed Subordinate CA and cross certificates are generated and issued in accordance with the CA's disclosed business practices; • upon issuance, complete and accurate Subordinate CA and cross certificates are available to relevant entities (Subscribers and Relying Parties) in accordance with the CA's disclosed business practices; • subordinate CA and cross certificates are revoked based on authorised and validated certificate revocation requests; and • timely, complete and accurate certificate status information (including CRLs and other certificate status mechanisms) is made available to any entity in accordance with the CA's disclosed business practices.		
	Subordinate CA (Sub-CA) and Cross Certificate Registration		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
7.1.1	The Parent CP specifies the requirements for submission of Sub-CA and cross certification requests.		
7.1.2	The Parent CA authenticates the Sub-CA or cross certificate request in accordance with the Parent's CP.		
7.1.3	The Parent CA performs an assessment of the Sub-CA or cross certificate applicant's compliance with the requirements of the Parent CA's CP before approving a Sub-CA or cross certificate request, or alternatively the Sub-CA or cross certificate applicant presents its CPS for assessment.		
	Sub-CA and Cross Certificate Renewal		
7.1.4	Where Sub-CA and cross certificate renewal is permitted, the Parent CA's CP specifies the requirements for submission of Sub-CA or cross certificate renewal requests.		
7.1.5	Where Sub-CA certificate and cross certificate renewal is permitted, the Parent CA authenticates the Sub-CA or cross certificate renewal request in accordance with the CA's CP.		
	Sub-CA and Cross Certificate Rekey		
7.1.6	The Parent CA's CP specifies the requirements for submission of Sub-CA rekey requests.		
7.1.7	The Parent CA authenticates the Sub-CA certificate rekey request in accordance with the CP.		
	Sub-CA and Cross Certificate Issuance		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
7.1.8	The Parent CA generates certificates: a) using the appropriate certificate profile in accordance with the CP and ISO 9594/X.509 and ISO 15782-1 formatting rules; b) with the validity periods formatted in accordance with ISO 9594/X.509, ISO 15782-1 and the CP; and c) where extensions are used, with extension fields formatted in accordance with ISO 9594/X.509, ISO 15782-1 and the CP.		
7.1.9	The Parent CA signs the Sub-CA or cross certificate with the Parent CA's private signing key.		
	Sub-CA and Cross Certificate Distribution		
7.1.10	The Parent CA makes Sub-CA and cross certificates available to relevant entities (e.g., Relying Parties) using an established mechanism (e.g., a repository such as a directory) in accordance with the Parent CA's CP.		
	Sub-CA and Cross Certificate Revocation		
7.1.11	The Parent CA verifies the identity and authority of the entity requesting revocation of a Sub-CA or cross certificate in accordance with the Parent CA's CP.		
7.1.12	The Parent CA updates the Certificate Revocation List (CRL) and other Sub-CA or cross certificate status mechanisms upon certificate revocation in accordance with the Parent CA's CP.		
	Sub-CA and Cross Certificate Status Information Processing		

Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
7.1.13	The Parent CA makes Sub-CA and cross certificate status information available to Relying Parties using an established mechanism (e.g., CRL, OCSP, etc.) in accordance with the Parent CA's CP.		

Controls based on WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security

Criteria related to SSL Baseline Requirements Business Practices Disclosure

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
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	Client ABC-CA's CPS is made publicly available to subscribers and any relying parties. It covers but is not limited to the topics in RFC 3647.		
		Client ABC-CA's CAs are operated in accordance with the WebTrust for Certificate Authority criteria and the latest version of the CA/Browser Forum Baseline Requirements. During each annual documentation review, the latest versions of these standards are reviewed, and internal documentation is aligned with updates that may apply.		
		Client ABC-CA makes its Intermediate CA certificate available from the Client A web site. The exact location is linked from the CPS.		
		On a monthly basis Client ABC-CA monitors the requirements set forth by relevant Root programs and adapts its procedures and practices as necessary.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	CA/Browser Forum.			
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.	Client ABC-CA's CPS is made publicly available to subscribers and any relying parties. It covers but is not limited to the topics in RFC 3647.		
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.	Client ABC-CA's CPS is made publicly available to subscribers and any relying parties. It covers but is not limited to the topics in RFC 3647.		
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	The CPS is reviewed against the latest version of the Baseline Requirements and is approved by the CA Policy Authority and Client ABC-CA's legal team at least annually.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	Requirements are updated annually.			
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 and include all material required by RFC 3647.	The CA Policy Authority has final authority and responsibility for approving the Certification Practices Statement, all operational procedures, and the Inventory documentation. All revisions to the CPS are numbered and relevant parties are informed of updates through Client ABC-CA's web site.		
		Client ABC-CA's CPS is made publicly available to subscribers and any relying parties. It covers but is not limited to the topics in RFC 3647.		
		The CPS is reviewed against the latest version of the Baseline Requirements and is approved by the CA Policy Authority and Client ABC-CA's legal team at least annually.		
6	The CA discloses in its Certificate Policy (CP) and/or Certification Practices Statement (CPS) under section 4.2 its policy or practice on processing CAA (Certification Authority Authorisation) DNS Records for Fully Qualified Domain Names that is consistent with the SSL Baseline Requirements, and	Client ABC-CA's CPS discloses under section 4.2 the CA's practice for processing CAA DNS records in adherence to the latest version of the Baseline Requirements.		
		Client A stores all issuance or revocation events in an audit log. Events are transferred from the Certificate Authority server to a log server over SSL, which then writes the logs into the log storage system. Certificate Authority personnel do not have write access to log storage system entries. Audit logs include certificate issuance and		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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.	revocation, key generation and logins by trusted personnel.		
7	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.	Contact information for the Policy Authority is available within Client ABC-CA's CPS which made publicly available to subscribers and any relying parties.		
8	The CA has controls to provide reasonable assurance that public access to its repository is read-only.	All public versions of Client ABC-CA's CPS are available online on Client ABC-CA's PKI website. Public access to the CPS repository is read-only.		

Criteria related to SSL Baseline Requirements SSL Service Integrity

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	Key Generation Ceremonies			
1.1	The CA maintains controls to provide reasonable assurance	ABC-CA key ceremonies follows a formal key generation script in		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	that Root CA and Subordinate CA Key Pairs are created in accordance with SSL Baseline Requirements Section 6.1.1.1.	accordance with WebTrust for CA 4.1 ABC-CA engages a Qualified Auditor to witness and opine on its key generation ceremonies in accordance with WebTrust for CA 4.1 ABC-CA key pairs are generated in a physically secured and controlled environment in accordance with WebTrust for CA 3.4. ABC-CA key pairs are generated within secure cryptographic modules in accordance with WebTrust for CA 4.1.		
	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.	ABC-CA CA software is configured to generate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.		
2.2	The CA maintains controls to provide reasonable assurance that the version of certificates issued are of type x.509 v3.	ABC-CA CA software in configured to generate x509 v3 certificates.		
2.3	The CA maintains controls to provide reasonable assurance that the extensions,	ABC-CA CA software in configured to generate x509 v3 certificates.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Root CA certificates generated conform to the Baseline Requirements.			
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.	ABC-CA CA software in configured to generate x509 v3 certificates.		
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.	ABC-CA CA software is configured to generate certificates conforming to the current versions of the Baseline Requirements and its CP/CPS at time of issuance, including extensions, key sizes, and policy identifiers.		
2.6	The CA maintains controls to provide reasonable assurance that with exception to the requirements	ABC-CA CA software is configured to generate RFC-5280 compliant certificates, except where Baseline Requirements specifies otherwise.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	stipulated in the Baseline Requirements 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.			
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.	ABC-CA CA software is configured to not issue subscriber certificates with a validity period longer than 825 days.		
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	ABC-CA CA software is configured to generate certificates conforming to the current versions of the Baseline Requirements and its CP/CPS at time of issuance.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	data in public context			
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	The contents of ABC-CA certificates are reviewed by a Verification Specialist and Manager for conformance to the Baseline Requirements and its CP/CPS prior to issuance.		
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.	ABC-CA CA software is configured to not use the SHA-1 hash algorithm.		
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.	ABC-CA CA software is configured to compare the Issuer DN of the generated certificate to the subject DN of the issuing CA and only successfully issue the certificate if there is a match.		
2.12	The CA maintains controls to provide reasonable assurance that for Subscriber certificates issued:	ABC-CA CA software is configured to ensure: • The subjectAltName extension is present and contains at least one entry		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	• 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	• 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.		
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.	ABC-CA CA software performs automated verification of the subjectAltName and subject:commonName fields to determine that Reserved IP Addresses or Internal Names are not included. The contents of ABC-CA certificates are reviewed by a Verification Specialist and Manager for conformance to the Baseline Requirements and its CP/CPS prior to issuance.		
2.14	The CA maintains controls to provides reasonable assurance that: • All certificates with a validity period of more than 30 days are revoked as of 15 January 2019; • Prior to 1 April 2019, certificates	ABC-CA CA software is configured to automatically reject certificates containing underscore characters in dNSNames.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	containing underscore characters ("_") domain labels in dNSName entries MAY be issued as follows: o dNSName entries may include underscore characters such that replacing all underscore characters with hyphen characters ("-") would result in a valid domain label, and; o Underscore characters are not placed in the left most domain label, and; o Such certificates are not valid for			

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	longer than 30 days • As of 1 April 2019, the CA does not issue certificates with underscore ("_") characters in dNSName entries; and • As of 1 May 2019, there are no valid certificates with underscore ("_") characters in dNSName entries.			
2.15	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	ABC-CA CA software is configured to generate certificates conforming to the current versions of the Baseline Requirements and its CP/CPS at time of issuance. The contents of ABC-CA certificates are reviewed by a Verification Specialist and Manager for conformance to the Baseline Requirements and its CP/CPS prior to issuance.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	• subject:postalCode • subject:countryName • subject:organizationalUnitName • Other Subject Attributes • Subject field requirements if Reserved Certificate Policy Identifiers are asserted • Subject Information for Root and Subordinate CA certificates			
2.16	The CA maintains controls to provide reasonable assurance that Subordinate CA certificates technically constrained using the nameConstraints extension conform to the Baseline Requirements.	ABC-CA CA software is configured that name-constrained Subordinate CA certificates conform to the Baseline Requirements.		
2.17	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,	ABC-CA CA software is configured to reject certificates containing known weak keys and other malformed keys.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	6.1.6, or if it has a weak Private Key (such as a Debian weak key).			
	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.	Subscribers are required to submit a certificate signing request and agree to the Subscriber Agreement prior to the issuance of a certificate.		
3.2	The CA maintains controls to provide reasonable assurance that the Certificate Request is: • obtained and complete prior to the issuance of Certificates;	Certificate requests are obtained and prior the issuance of the certificate they are: • signed by the authorized individual (Certificate Requestor) • properly certified as to being correct by the applicant		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	• 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.	and contains the information specified in Section 4.2.1 of the SSL Baseline Requirements		
	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.	Private key for any subscribers or subordinate CAs are encrypted for transportation when generated by the CA.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	• 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.			
	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	Subscribers are required to agree to the Subscriber Agreement through the CA's certificate application process prior to the issuance of a certificate. The		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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.	Subscriber agreement contains provisions imposing obligations and warranties as stated in the CA's CP/CPS.		
	Verification Practices			
	Verification of Domain Control			
4.1	The CA maintains controls to provide reasonable assurance	Authorization for using Fully-Qualified Domain Names (FQDNs) in a certificate request are validated by the CA in		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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.	accordance with one of the method listed in SSL Baseline Requirements Sections related to the Fully- Qualified Domain Name(s) prior to issuance (including wildcard domains and new gTLDs (generic top-level domains)) and IP address(es) listed in the Certificate.		
	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	Certificate requests are vetted in accordance with SSL Baseline Requirements – Subject Identity requirements (SSL Baseline Requirements Section 3.2.2.1), including:		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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)	• 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)		
4.3	The CA maintains controls to provide reasonable assurance that it inspects any document relied upon for identity confirmation for alteration or falsification.	Identity information is vetted against approved reliable data sources.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
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 CA SHALL provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.	A list of authorized certificate requesters is obtained during the subscriber registration (application) process.		
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.	The subjectcountryName field when present, is screened in order to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located.		
4.6	The CA maintains controls to provide reasonable assurance that the CA does not	Initial identity validation requirements (as defined the SSL Baseline Requirements) used for certificate requests are		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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. And, validations completed using methods specified in Section 3.2.2.4.1 or Section 3.2.2.4.5 are not re-used on or after 1 August 2018.	revalidated every 825 days prior to issuing a certificate.		
4.7	The CA maintains controls to provide reasonable assurance that the CA uses an internal database of all previously revoked	Certificate requests are checked against an internal database of all previously revoked certificates and previously rejected certificates due to suspected phishing or other fraudulent		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns to identify subsequent suspicious certificate requests.	usage or concerns to identify subsequent suspicious certificate requests.		
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.	Documented procedures for High Risk Certificates are defined and implemented that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified.		
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.	Data sources are evaluated for its reliability, accuracy, and resistance to alteration or falsification prior to being considered as a reliable data source by the CA.		
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	CAA (Certificate Authority Authorisation) records are checked, and, if present, the associated records are processed and the certificate(s) are issued in accordance with the requirements set forth in Section 3.2.2.8 of the SSL Baseline Requirements.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	checks for CAA (Certificate Authority Authorisation) records, and, if present, processes these records and issues certificates in accordance with the requirements set forth in Section 3.2.2.8 of the SSL Baseline Requirements.			
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.	Potential certificate issuances that were prevented by CAA record are logged with details to provide feedback to the CA/Browser Forum on the circumstances.		
	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 issuance by a Root CA follow a documented key ceremony process, and is administered by individual authorized CA system operator (with a witness) to deliberately issue a direct command, in order for the Root CA to perform a certificate signing operation.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	certificate signing operation.			
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.	Root CA private keys are used to sign certificates in the following cases: • Self-signed Certificates to represent the Root CA itself; • Certificates for Subordinate CAs and Cross Certificates; • Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and Certificates for OCSP Response verification		
	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 Certificate Problem Requests, and that the CA provides a process for Subscribers to request revocation of their own certificates.	• The CA maintains a web-based form that allows for 24x7 availability to accept Certificate Problem Requests and automated tickets are created to respond to requests timely. • The CA provides subscribers with a web-based application to support authentication and indicate revocation of certificates.		
5.2	The CA maintains controls to provide reasonable assurance that it: • has the capability to	The CA maintains a web-based form that allows for 24x7 availability to accept Certificate Problem Requests and automated tickets are created to respond to requests timely.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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 SSL Baseline	The ticketing system assigns a high priority to certificate problem requests and notifies the proper level of support to begin an investigation within 24 hours of receipt. The CA begins investigations of Certificate Problem Reports within 24 hours and provides a preliminary report on its findings to both the Subscriber and the entity who filed the Report when it becomes available. Upon completion of a Certificate Problem Report investigation, 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 specified in Section 4.9.1.1 of the SSL Baseline Requirements and is logged by the ticketing system.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	Requirements 4.9.1.1; and • where appropriate, forwards such complaints to law enforcement.			
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	The CA provides subscribers with a web-based application to support authentication and indicate revocation of certificates. Subscriber certificates are revoked automatically within 24 hours in the occurrence of a subscriber-initiated request from the web-based application. In the event described in WTBR 2-5.3, subscriber revocations are tracked in the ticketing system and revoked timely. Subscriber certificates are revoked within 5 days in the		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	4. 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 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;	occurrence of any event described in WTBR 2-5.3.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	4. The CA is made aware of any circumstance indicating that use of a FullyQualified 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;			

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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;			

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	10. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or 11. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed.			
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:	Subordinate CA Certificates are revoked within 7 days in the occurrence of any event described in WTBR 2-5.4.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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			

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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			

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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 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	The CA makes revocation information available via the cRLDistributionPoints certificate extension for Subordinate CA and Subscriber Certificates. The CA makes revocation information available via the authorityInformationAccess certificate extension for Subordinate CA and Subscriber Certificates. For high-traffic Fully Qualified Domain Names, the CA distributes its OCSP responses in accordance with SSL Baseline Requirements.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	SSL Baseline Requirements.			
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	The CA maintains an online repository with 24x7 availability that application software can use to automatically check the current status of all unexpired Certificates issued by the CA. For the status of Subscriber Certificates, CRLs are configured to update and reissue 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 based on approved templates or scripts. For Subscriber Certificates, information provided via an OCSP is configured to updated 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, CRLs are configured to update and reissue 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 based on approved templates or scripts. For Subscriber Certificates, information provided via an OCSP is configured to updated at least every four (4) days and OCSP responses must have a maximum expiration time of ten (10) days.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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	For subordinate CA Certificates, CRLs are configured to update and reissue at least once every twelve (12) months and within 24 hours after revoking a subordinate CA certificate. The value of the nextUpdate field must not more than twelve months beyond the value of the thisUpdate field. For subordinate CA Certificates, information provided via an OCSP is updated at least every twelve (12) months and within 24 hours after revoking a subordinate CA Certificate. Revocation information is available through an OCSP capability using the GET method for Certificates issued in accordance with the SSL Baseline Requirements.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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			

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	the SSL Baseline Requirements.			
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.	The CRL operated by the CA are subject to automated monitoring to test response times of ten seconds or less under normal operating conditions.		
		The OCSP Responder operated by the CA is subject to automated monitoring to test response times of ten seconds or less under normal operating conditions.		
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.	The CA configures CRLs to remove revocation entries on a CRL until after the Expiry Date of the revoked certificate.		
		The CA configures CRLs to remove revocation entries on a CRL until after the Expiry Date of the revoked certificate.		
5.9	The CA maintains controls to provide reasonable assurance that OCSP responses conform to RFC6960	The CA maintains an OCSP responder to respond to OCSP requests. The OCSP responder is implemented by an RFC 5019-compliant server, backed by a local repository of known		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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).	certificate serial numbers and statuses. Responses to OCSP requests are signed with an OCSP certificate signed by the CA.		
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.	The OCSP Responder software is configured to not respond with a "good" for certificates which have not been issued by the CA.		
	EMPLOYEES AND THIRD PARTIES			
6.1	The CA maintains controls to verify the	ABC-CA maintains controls to provide reasonable assurance that		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	identity and trustworthiness of an employee, agent, or independent contractor prior to engagement of such persons in the Certificate Management Process.	personnel and employment practices enhance and support the trustworthiness of the CA's operations. On an annual basis, personnel are trained, and successful completion of the training is registered. Where legally permitted, ABC-CA conducts background checks on new employees. Employees are continuously evaluated during performance reviews.		
		ABC-CA provides CA specific training information to new employees who work in a trusted role within the CA environment to ensure they are aware of the procedures and policies that apply to their respective position. Training is repeated annually, and attendance is registered. Engineers must complete an examination prior to being able to issue certificates.		
		Engineers must formally request authorization to access CA systems and the CA facilities, and require approval from the CA Policy Authority. Engineers must be formally de-registered once they no longer require access. The departed user's account is removed from the CA systems and from relevant groups within four (4) days of the date on which the user has left the CA Organization.		
6.2	The CA maintains controls to provide reasonable assurance that:	ABC-CA maintains controls to provide reasonable assurance that personnel and employment practices enhance and support the		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	• 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	trustworthiness of the CA's operations. On an annual basis, personnel are trained, and successful completion of the training is registered.		
		Where legally permitted, ABC-CA conducts background checks on new employees. Employees are continuously evaluated during performance reviews.		
		ABC-CA provides CA specific training information to new employees who work in a trusted role within the CA environment to ensure they are aware of the procedures and policies that apply to their respective position. Training is repeated annually, and attendance is registered. Engineers must complete an examination prior to being able to issue certificates.		
		Engineers must formally request authorization to access CA systems and the CA facilities, and require approval from the CA Policy Authority. Engineers must be formally de-registered once they no longer require access. The departed user's account is removed from the CA systems and from relevant groups within four (4) days of the date on which the user has left the CA Organization.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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.			
6.3	The CA maintains controls to provide reasonable assurance that before the CA authorizes a Delegated Third Party to perform a delegated function,	N/A - Not Applicable for the Client A CA Environment as Client A does not use delegated third party personnel to issue certificates.	N/A	N/A

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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.			

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
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.	N/A - Not Applicable for the Client A Trust Services CA Environment as Client A does not use delegated third party personnel to issue certificates.	N/A	N/A
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.	N/A - Not Applicable for the Client A Trust Services CA Environment as Client A does not use delegated third party personnel to issue certificates.	N/A	N/A
6.6	The CA maintains controls to provide reasonable assurance that the CA internally audits each Delegated Third Party's compliance with the Baseline	N/A - Not Applicable for the Client A Trust Services CA Environment as Client A does not use delegated third party personnel to issue certificates.	N/A	N/A

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	Requirements on an annual basis.			
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.	Client ABC-CA's CAs are operated in accordance with the WebTrust for Certificate Authority criteria and the latest version of the CA/Browser Forum Baseline Requirements. During each annual documentation review, the latest versions of these standards are reviewed, and internal documentation is aligned with updates that may apply.		
	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.	Any certificate request is validated according to certificate issuance procedures, which includes validating ownership of the Common Name, and the authority of the requester. Certificates issued can be tracked back to a ticket in the ticketing system. Requests must be made in compliance with the CPS.		
		Client A stores all issuance or revocation events in an audit log. Events are transferred from the Certificate Authority server to a log server over SSL, which then writes the logs into the log storage system. Certificate Authority personnel do not have write access to log storage system entries. Audit logs include certificate issuance and		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
		revocation, key generation and logins by trusted personnel.		
		All tickets and log records related to the request verification, issuance or revocation of a certificate is kept for a total of at least seven (7) years after the expiration time of that certificate.		
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	Client A stores key lifecycle management, CA and Subscriber Certificate lifecycle management events, and security events in an audit log that is retained for at least seven years. Certificate Authority personnel do not have write access to log entries.		
		An audit trail of all access to the CA facilities is maintained which is tracked in an audit log. All access to the CA systems is recorded in both physical access logs and in the formal approval process signed off by the CA Policy Authority and are retained for at least seven years.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	requests, and revocation ○ all verification activities stipulated in the Baseline Requirements and the CA's Certification Practice Statement ○ date, time, phone number used, persons spoken to, and end results of verification telephone calls ○ acceptance and rejection of certificate requests ○ issuance of Certificates ○ generation of Certificate Revocatio			

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	n Lists (CRLs) and OCSP entries. • security events, including: ○ successful and unsuccessful PKI system access attempts ○ PKI and security system actions performed ○ security profile changes ○ system crashes, hardware failures, and other anomalies ○ firewall and router activities ○ entries to and exits from CA facility. • Log entries must include the following elements:			

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	○ Date and time of entry ○ Identity of the person making the journal entry ○ Description of entry			
7.3	The CA maintains controls to provide reasonable assurance that audit logs generated are retained for at least seven years.	All tickets and log records related to the request verification, issuance or revocation of a certificate is kept for a total of at least seven years after the expiration time of that certificate.		
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.	All tickets and log records related to the request verification, issuance or revocation of a certificate is kept for a total of at least seven years after the expiration time of that certificate.	.	
	AUDIT			
8.1	The CA maintains controls to provide reasonable assurance that for Subordinate CAs that are considered technically constrained in	N/A - Not Applicable for the Client A Trust Services CA environment as Client A does not have any Subordinate CAs that are considered technically constrained in accordance with	N/A	N/A

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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.	SSL Baseline Requirements Section 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	The CA infrastructure is audited annually against the WebTrust Principles and Criteria for Certification Authorities as well as the CA/Browser Forum SSL Baseline Requirements. Client A publishes the audit report in a public repository and shares it		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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.	with external stakeholders where required or contractually agreed upon.		
		On an annual basis Client A requests the latest audit report from all externally operated subordinate CAs which are cross-signed by a Client A CA. Based on the report, Client A validates that the concerned subordinate CAs meet the relevant compliance requirements.		
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	N/A - Not Applicable for the ABC-CA CA Environment as client does not use delegated third party personnel to issue certificates.	N/A	N/A

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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	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	On a quarterly basis, ABC-CA assigns an auditor who verifies at least 10% of all certificates issued during the period commencing immediately after the previous audit for compliance with the CA/Browser Forum requirements. In addition, the auditor reviews all certificate requests by CA personnel to ensure that the requests are valid and appropriate. Audit results are tracked in a ticket, and approved by the CA Policy Authority, who decides on the need for remedial action if needed.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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.			
8.5	The CA maintains controls to provide reasonable assurance that it complies with:	Changes to ABC-CA's control documentation and CPS are reviewed and approved by Client ABC-CA's legal team and the		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	• 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.	CA Policy Authority to ensure they meet relevant statutory, legal and contractual requirements. All contracts relevant to CA operations are reviewed by ABC-CA's legal team prior to signing.		

Criteria Related to CA Environmental Security

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
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	ABC-CA 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		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	• comply with all other security requirements applicable to the CA by law.	Management Processes; and • comply with all other security requirements applicable to the CA by law. ABC-CA reviews and updates its security program at least annually.		
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	ABC-CA performs an annual risk assessment 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		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	that the CA has in place to counter such threats.	the CA has in place to counter such threats.		
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.	ABC-CA 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		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
		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;	ABC-CA develops, implements, and maintains a Business Continuity Plan that includes: • 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;		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	• 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.[8]	• 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 ABC-CA Business Continuity Plan is tested at least annually, reviewed, and updated.		
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);	ABC-CA's Certificate Management Process conforms to WebTrust for CA, including: • physical security and environmental controls (see WTCA 2.0 Section 3.4); • system integrity controls, including		

[8] 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.

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	• 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); • 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).	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); • 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	Refer to WTCA 3.4 Illustrative Controls		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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.			
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.	Refer to WTCA 3.7 Illustrative Controls		
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	Refer to WTCA 3.6 Illustrative Controls		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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.			
9	The CA maintains controls to provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations.	Refer to WTCA 3.3 Illustrative Controls		
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	Refer to WTCA 3.10 Illustrative Controls		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	archived audit logs are maintained; • audit logs are completely and confidentially archived in accordance with disclosed business practices; and • 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	Refer to WTCA 3.4 and 4.2 Illustrative Controls		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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.			
12	The CA maintains controls to provide reasonable assurance that it enforces multi-factor authentication for all accounts capable of directly causing certificate issuance.	ABC-CA CAs are configured to require multi-factor authentication for all accounts capable of directly causing certificate issuance		

Criteria Related to Network and Certificate System Security Requirements

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
1.1	The CA maintains controls to provide reasonable assurance that certificate Systems are segmented into networks based on their functional, or logical relationship.	CA systems are segregated into high and medium security zones. Logical segregation is achieved through network segregation, using virtual segregation (VLAN), and by controlling network access through firewall rules.		
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.	Security hardening and baseline configuration standards for PKI servers have been established according to industry standards and are reviewed and updated periodically. Mechanisms to detect deviations from baseline configurations are applied on PKI servers. Deviations are tracked to resolution.		
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.	Root CA systems that do not issue end-entity certificates or that do not have business need to be online are air gapped from any		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
		corporate or public network.		
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.	CA systems at primary and backup CA facilities are hosted in a physically isolated secure rack with dual-control and multi-factor authentication.		
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.	PKI systems are segregated into high and medium security zones. Logical segregation is achieved through network segregation, using virtual segregation (VLAN), and by controlling network access through firewall rules.		
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.	Network traffic to and from untrusted networks passes through a policy enforcement point; firewall rules are established in accordance to identified security requirements and business justifications.		
1.7	The CA maintains controls to provide reasonable assurance that Issuing Systems, Certificate Management	Default administrator accounts and guests' accounts are		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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.	disabled or renamed prior to deployment in production.		
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.	Security hardening and baseline configuration standards for PKI servers have been established according to industry standards and are reviewed and updated periodically. Mechanisms to detect deviations from baseline configurations are applied on PKI servers. Deviations are tracked to resolution.		
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.	Privileged access to the certificate system hosts is restricted to authorized individuals and reviewed quarterly.		
1.10	The CA maintains controls to provide reasonable assurance	Multi-factor authentication to CA		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	that Multi-Factor Authentication is implemented to each component of the Certificate System that supports Multi-Factor Authentication.	systems is enforced via Smartcard and PIN.		
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.	Privileged access to certificate systems is revoked within 24 hours. Access revocation is documented and any CA assets are collected upon termination of employment or role change.		
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.	Security-relevant patches, including software or firmware updates are applied to Certificate systems on periodic cadence. Security patches that introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch are documented.		
	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	Trusted and authorized roles are defined and documented in the CP/CPS. A formal		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	responsibilities to them is followed.	review of membership of trusted and authorized roles is performed annually.		
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.	Management has defined and implemented an organization division of Trusted Roles and Responsibilities, which reduces the risk of a single individual having the opportunity to subvert critical processes.		
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.	Physical access is restricted to only authorized individuals in physical data center environments.		
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.	Roles and responsibilities for the governance of CAs PKI are formally documented within the Trusted Roles and Responsibilities Standard and communicated on the intranet.		
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.	Logical access provisioning to Certificate systems requires approval from appropriate personnel. Access privileges are based on the job		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
		responsibility for the Trust Role prior to assigning access privileges.		
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.	The use of "Non-user domain accounts" or "shared accounts" for certificate enrollment and/or interactive logon, shall go through a risk acceptance signoff. Authentication credentials for shared and group accounts are reset every 90 days.		
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 authentications which cross a zone boundary into a Secure Zone or High Security Zone: o Require Multi-Factor Authentication • For accounts accessible from outside a Secure	Password policies have been implemented to enforce applicable length and complexity based on the assessed security of the zone.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	Zone or High Security Zone: o 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.	Multi-Factor Authentication is implemented for all CA systems based on the applicable zone.		
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.	The CA maintains a written policy requiring Trusted Roles to log out of or lock workstations when no longer in use.		
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.	CA domain policy is configured enforce inactivity timeout features.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
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.	Workstations are configured with Inactivity timeouts that lock workstations after a set period of inactivity.		
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.	CA domain policy is configured enforce inactivity timeout features.		
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.	All system accounts are reviewed and documented every three months by the network administrator and accounts no longer necessary for operations are deactivated.		
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	The certificate systems domain are configured with prescribed lockout settings based on an approved number of		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	access attempts, provided that: • This security measure is supported by the Certificate System; and Does not weaken the security of this authentication control.	unsuccess attempts based on security assessments.		
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.	Upon a change in role a ticket is created to document access to Certificate Systems being revoked within 24 hours of role change.		
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.	Multi-Factor Authentication is implemented for all CA systems based on the applicable zone.		
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.	Multi-party authentication is required to gain physical or logical access directly to the CA.		
2.14	The CA maintains controls to provide reasonable assurance that it enforces Multi-Factor	Multi-Factor Authentication is implemented for all		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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.	CA systems based on the applicable zone.		
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	Remote administration access to Issuing Systems, Certificate Management Systems, and Security Support Systems is restricted, except for the situations described in WTBR 4-2.15.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	Mediates the remote connection to the Issuing System.			
	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.	Security Support Systems are implemented to monitor, detect, and report any security-related configuration changes on Certificate Systems.		
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.	Certificate Systems capable of monitoring and logging system activity are configured to continuously monitor and log system activity.		
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.	Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when defined thresholds are reached.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
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.	Electronic intrusion detection systems are configured to monitor, detect, and automatically alert appropriate personnel of Critical Security Incidents.		
3.4	The CA maintains controls to provide reasonable assurance that Trusted Role personnel follows up on alerts of possible Critical Security Events.	Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution.		
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	Trusted Role personnel follow up on alerts of possible Critical Security Events within defined timelines.		
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:	A human review of application and system logs is performed and documented in the ticketing system		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	• Validating the integrity of logging processes; and Testing the monitoring, logging, alerting, and log-integrity-verification functions are operating properly.	monthly and includes validating the integrity of logging processes and testing that monitoring, logging, alerting, and log-integrity-verification functions are operating properly.		
3.6	The CA maintains controls to provide reasonable assurance that it maintains, archives, and retains logs in accordance with its disclosed business practices.	Logs are configured to be maintained, archived, and retained in accordance with disclosed business practices.		
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	Monthly human log reviews include determining logs are maintained based on defined retention periods.		

Criteria	WebTrust Baseline Criteria	Controls specified by ABC-CA	Tests of Controls Performed	Results of Tests
	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.			

Section 5

Other Information Provided by ABC-CA That Is Not Covered by the Service Auditor's Report

This section will discuss issues that were identified in the audit (or reported to Bugzilla) for which management wants to discuss the remediation that has been undertaken or is planned to be undertaken.