COMPLIANCE AUDIT CHECKLIST

1. Certificate Authority Overall Governance

S/No	Control Steps	Checks
Obligations to Subscribers, Relying Party and User Community		
1	**User Community Obligation** The Auditor shall review that the Certification Authority (CA) has informed the User Community of: 1. The CA's procedures for certificate registration, issuance, suspension and revocation; 2. Any *force majeure* that relieves the CA of its duties; 3. The time-intervals between each update and publication of the certificate suspension, revocation and Certification Revocation List (CRL) information; 4. The scope and limitations of the CA's liabilities with respect to the expected reliance to be placed in the information contained in the certificates; 5. The CA's Certificate Practice Statement (CPS) and Certificate Policies (CP). In addition, the Auditor shall review that: 1. The mode of communication should be reasonable to reach a majority of the User Community; 2. All updates are within the established time-intervals defined by the CA.	1. Sight evidence that the CA has performed its obligation to the User Community as defined in the Control Step.
2	**Subscribers Obligation** The Auditor shall review that the CA has informed the Subscribers of their responsibility to validate the accuracy of the information contained in their certificates upon issuance. In addition, the Auditor shall review that: 1. Subscribers' explicit consent has been obtained before publication of their certificates on the repository; 2. The CA has informed the Subscribers on how the private keys have been protected.	1. Sight evidence that the CA has performed its obligation to the Subscribers as defined in the Control Step; 2. Sampled observations of Subscribers' acknowledgements on their responsibility; 3. Inquire the CA if any Subscribers' certificates are published and sight obtained consent.
3	**Relying Party Obligation** The Auditor shall review that the CA has informed the Relying Party on steps to be taken to verify the authenticity and validity of a certificate. The steps shall include but are not limited to the verification of: 1. Issuer's signature; 2. Policy parameters; 3. Usage parameters; 4. Validity period; 5. Revocation or suspension information; and 6. Reliance limit.	1. Sight evidence that the CA has performed its obligation to the Relying Party as defined in the Control Step.
Certificate Practice Statement (CPS) and Certificate Policies (CP)		
4	The Auditor shall review that the CA has prepared its CP and CPS using guidelines stated in IETF's *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* (RFC 3647).	1. Inquire the CA on how they prepared the CP and CPS using RFC3647 as guidelines.

S/No	Control Steps	Checks
5	The Auditor shall review that the CP and CPS include the following: 1. Effective date; 2. Version number; 3. Change history; 4. Publication & Repository responsibilities; 5. CA's identification and authentication processes; 6. CA's Certificate Life-Cycle Operations; 7. Physical controls; 8. Procedural controls; 9. Personnel controls; 10. Technical security controls; 11. Audit trails; 12. Certificate and CRL profiles; 13. CA's self-assessment and external audit requirements; 14. Business and Legal matters; 15. Limited liability clauses. In addition, the Auditor shall review that each CP has been defined for each class of certificates. It is possible that all classes of certificates use the same CP.	1. Sight that the CP and CPS minimally contain the information as defined in the Control Step; 2. Sight that each CP has been defined for each class of certificate.
Security Management		
6	The Auditor shall review that an IT Security Policy exists and: • Is approved by the CA's management; • Is reviewed regularly; • Is communicated to, understood and acknowledged by personnel directly involved in the CA operations.	1. Sight the existence of an IT Security Policy; 2. Sight evidence that the IT Security Policy is approved and reviewed yearly; 3. Sampled observations of personnel acknowledgement forms which indicate they have read and understood the IT Security Policy.
7	The Auditor shall review that regular updates on security risks and exposures are communicated to personnel directly involved in the CA operations. The regular updates can be in the form of email, circulars, website updates or training.	1. Sampled observations of security risks and exposure updates communiqué.
8	The Auditor shall review that personnel responsible for security management have been trained by: 1. Inspecting qualifications/certifications such as CISSP or equivalent; OR 2. Inspecting if the personnel have attended training and the content of the training.	1. Observation of training records or certifications.
9	The Auditor shall review the access control matrixes and its follow-up actions on a regular basis.	1. Observation of monthly access control matrix review reports; 2. Sampled observations which indicate follow-up actions are implemented within 24 hours.

S/No	Control Steps	Checks
10	The Auditor shall review the existence and implementation of: 1. Vulnerability management procedures covering, but not limited to: a. sources of information; b. planning and execution of counter measures. 2. Incident management procedures covering, but not limited to: a. compromise of key; b. penetration of systems or network; c. unavailability of network; d. security incidents; e. fraudulent activities surrounding the registration, generation, suspension and revocation of certificates; f. informing the Controller within 24 hours of any incidents. In addition, the Auditor shall review that the CA has documented and acted on identified incidents.	1. Sight the existence of vulnerability management procedures and that they minimally contain the information as defined in the Control Step. 2. Sampled observations that the vulnerability management procedures are tested and reviewed at least once every 6 months. 3. Sight the existence of incident management procedures and that they minimally contain the information as defined in the Control Step. 4. Sampled observations that the incident management procedures are tested and reviewed at least once every 6 months. 5. Sampled observations of incident records and observations that follow-up actions have been performed.
Risk Management		
11	The Auditor shall review that the CA performs a regular risk assessment of its CA infrastructure, which includes: 1. Cryptographic algorithm and key parameters; 2. Physical security; 3. Operating system security; 4. Network security; 5. Application security; 6. PKI software.	1. Observation of risk assessment reports and that the assessment minimally covers the areas as defined in the Control Step; 2. Sampled observations that follow-up actions are implemented within 1 month; 3. Sight evidence that assessment is performed at least yearly or after major changes to CA infrastructure (involving more than 50% of core infrastructure).
12	The Auditor shall review that the CA has the following: 1. Risk Management Policy; 2. Risk Management Procedures. In addition, the Auditor shall review that the CA management review, update and approve the policy and procedures regularly.	1. Sight the existence of Risk Management Policy and Procedures; 2. Sight evidence that the IT Risk Management Policy is reviewed, updated and approved yearly; 3. Sight evidence that the IT Risk Management Procedures are reviewed, updated and approved half-yearly.
Personnel Controls		
13	The Auditor shall review that the CA has taken steps to verify that personnel to be employed for direct CA operations are subject to security screening. The security screening should cover: 1. Criminal history; 2. Bankruptcy status; AND 3. Personnel self-declaration on criminal and bankruptcy history. In addition, the Auditor shall review that the CA performs regular reviews of the security screening of personnel.	1. Sight security screening process documentation that the security screening minimally covers the areas as defined in the Control Step; 2. Sampled observations of security screening documents; 3. Sampled observations of personnel self declaration forms.

S/No	Control Steps	Checks
14	The Auditor shall review that: 1. All personnel involved in CA operations have signed a confidentiality agreement; 2. These confidentiality agreements are reviewed when the terms of their employment contracts change.	1. Sampled observations of confidentiality agreements; 2. Sampled observations that confidentiality agreements are reviewed during employment contract changes (hires and terminations).
15	The Auditor shall review that the CA has documented and implemented segregation of duties for key CA operational roles, including but not limited to: 1. Requestor – Approval; 2. Maker – Checker; 3. Administration – Security; 4. Operations – Security.	1. Sight access control matrixes that conflicting roles are not present; 2. Observation that system access controls are according to segregation of duties.
16	The Auditor shall review that the CA implements dual control to: 1. Root equivalent accounts to systems; 2. Administrative accounts to key applications.	1. Sight access matrix that personnel assigned to root accounts and administrative accounts have dual controls.
17	The Auditor shall review that the CA designs and implements job responsibilities and the corresponding access matrix (logical and physical). The job responsibilities and access matrix should be documented and contain: 1. Effective date and validity; 2. Role description and assignees; 3. Access control assigned (including physical security); 4. Training requirements. The job responsibilities and access matrix should include names of backups. In addition, the Auditor shall review that the CA reviews the job responsibilities and access matrix regularly.	1. Sight access control matrix that it minimally covers the areas as defined in the Control Step; 2. Sample observations that job responsibilities and access matrix are reviewed at least once every 3 months; 3. Observation that system access controls are according to assigned responsibilities.
Subscriber's data		
18	The Auditor shall review that the CA has designed and implemented steps to protect the confidentiality and privacy of the Subscribers' data, including transactional and historical data about the Subscribers' usage.	1. Sight the existence of procedures surrounding protection of Subscribers' data; 2. Sampled observations of protection mechanism.
19	The Auditor shall review that explicit permissions have been obtained from the Subscribers by the CA for third party disclosure.	1. Sampled observations of permissions obtained from Subscribers for third party disclosure.
Incident Management		
20	The Auditor shall review that the CA has an approved Incident Management Plan. The Plan should include, but is not limited to the following: 1. Key compromise (RA Key, CA certification Key); 2. Intrusion to systems and network; 3. Breach of physical security; 4. Infrastructure downtime; 5. Fraudulent activities surrounding certificate management. The Auditor shall also review that the CA has informed the Controller promptly for **confirmed** incidents.	1. Sight existence of an Incident Management Plan that minimally covers the areas as defined in the Control Step; 2. Sampled observations that the CA has informed the Controller within 24 hours for confirmed incidents.

S/No	Control Steps	Checks
21	The Auditor shall review that the CA has an approved Incident Response Action Plan. The Plan should include, but is not limited to the following: 1. Compromise control; 2. Revocation conditions and procedures(e.g. revocation of CA certificate in the event that the CA certification key is lost or compromised); 3. Notification Parties and procedures; 4. Service disruption procedures; 5. Audit trail protection and analysis; 6. Media and public relations. The Auditor shall also review that the CA has tested and trained personnel on usage of the Incident Response Action Plan.	1. Sight existence of an Incident Response Action Plan that minimally covers the areas as defined in the Control Step; 2. Sight evidence that the key personnel were trained on the Plan; 3. Sight evidence that the Plan is tested at least annually; 4. Sampled observations that the Plan is used for actual incidents.
Business Continuity Planning		
22	The Auditor shall review that the CA has the following plans available: 1. Business Continuity Plans; 2. Disaster Recovery (DR) Plans. The Plans should include 1. Continuity plans in the event of CA certification key loss or compromise; 2. Named personnel in the recovery team; 3. The availability of cold backups (redundant systems); 4. Location of the DR site; 5. Backup procedures for use in the event of *force majeure* not being excluded from their obligations. In addition, the Auditor shall review that the Plans have been tested and inadequacies were rectified.	1. Sight existence of a Business Continuity Plan that minimally covers the areas as defined in the Control Step; 2. Sight existence of a Disaster Recovery Plan that minimally covers the areas as defined in the Control Step; 3. Sampled observations that Plans are tested and reviewed at least once every 6 months; 4. Sample observations that inadequacies in the Plans are rectified.
23	The Auditor shall review that the named personnel in the recovery team have been trained in the execution of the Plans.	1. Sampled observations of Plan training records of recovery team.
24	The Auditor shall review that the cold backups of the hardware used in the Plans are available and accessible.	1. Sight sampled cold backups can be started.
25	The Auditor shall review that the DR site has basic security (physical and environmental) in place.	1. Inquire the CA on security controls in place at DR site; 2. Sampled observations of security controls in DR site.

2. Certificate Management Controls

S/No	Control Steps	Checks
26	The Auditor shall review that the following exists as certificate attributes: 1. Certificate policy; 2. Usage parameters; 3. Expiration parameters; 4. Distinction between CA certificate and user certificate. In addition, the Auditor shall review that the following information do not exist: 1. Distinguished name fields; 2. Other information of users that may be used in social engineering.	1. Observation of sampled certificates that have certificate attributes as defined in the Control Step.
Registration Process		
27	The Auditor shall review that the CA has defined and implemented authentication methods to verify the certificate applicant. The Auditor shall also review that the authentication documents used are retained.	1. Sight authentication procedures; 2. Sample certificates issued by the CA and sight corresponding authentication documents.
Generation Process		
28	The Auditor shall review that the procedures adhered to in the generation process are in accordance to the CP.	1. Sampled observations of evidence that the generation process is carried out in accordance to the CP.
29	The Auditor shall review that the: 1. Information in the certificate is the same as in the request; 2. The correct key pair is associated with the certificate information.	1. Sampled comparisons that request information is the same as in the generated certificates; 2. Sight evidence that the correct key pair is associated with the certificate information.
Issuance Process		
30	The Auditor shall review that the issuance channel used for the transmission of certificate, passwords and private keys between the CA and Subscribers is secure. In addition, the Auditor shall review that receipt of certificates is acknowledged and accepted by the Subscribers.	1. Inquire the CA on protection mechanisms used for the transmission of certificates; 2. Sampled observations of the implemented protection mechanisms; 3. Sampled observations of acknowledgements of receipt and acceptance by Subscribers.
Publication Process		
31	The Auditor shall review that the CA has published its certificate, CP, CPS and repository in a secure channel. In addition, the Auditor shall review that the following information is available for the User Community to verify: 1. Company Name; 2. Registration number; 3. X500 name; 4. Internet address; 5. Telephone number; 6. CA certificate; 7. Location of repository.	1. Inquire the CA on protection mechanisms used for publication; 2. Sampled observations of the implemented protection mechanisms; 3. Sight that the information is available for the User Community and minimally contains the information defined in the Control Step.
32	The Auditor shall review that the CA obtained explicit consent for publication of Subscriber's certificate information.	1. Sampled observations of consent given for certificate information that was published.

S/No	Control Steps	Checks
33	The Auditor shall review that access to the repository: 1. Is read-only to the public, Subscribers and User Community; 2. Has restricted access to the CA's assigned personnel for updating the repository. In addition, the Auditor shall review that the modifications to the CPS are subject to a change management procedure of request and approval.	1. Inquire the CA on access controls to the repository; 2. Sampled observations of the implemented access controls; 3. Sampled observations of change management request and approval forms.
Renewal Process		
34	The Auditor shall review that the renewal requests are submitted using a secure channel OR using the same authentication method in the registration process.	1. Observation of security mechanism of renewal channel; 2. Inspection of sampled renewal requests for evidence that the secure renewal channel is used.
Certificate Suspension Process		
35	The Auditor shall review that suspended certificates are re-activated by the CA after investigations have completed and no compromise has been confirmed.	1. Sampled observations of re-activated certificates have supporting documents that indicate no compromise has taken place.
36	The Auditor shall review that the CA has taken steps to verify the identity of the requestor of certificate suspension.	1. Sampled observations of identity verification documents.
37	The Auditor shall review that information of suspended certificates are updated in the CRL and are digitally signed by the CA.	1. Sight evidence that the CRL is updated within 1 hour upon verification that suspension request is valid; 2. Sight updates include reason and date/time of suspension; 3. Sight all updates are digitally signed by the CA.
38	The Auditor shall review that the CA has taken steps to ensure that the suspension information in the CRL is protected from unauthorized modifications.	1. Inquire the CA on protection mechanisms used to prevent unauthorized modifications of suspension information; 2. Sampled observations of the protection mechanisms.
39	The Auditor shall review that the CA has informed the Subscriber of suspension.	1. Sampled observations of communication to Subscribers.
Revocation Process		
40	The Auditor shall review that the CA revokes the certificate when: 1. Information marked with extension "critical" is inaccurate; 2. Private key or media holding the private key is suspected or actually compromised; 3. Subscriber is no longer a member of the community subject to CP; 4. The Subscriber requests it; 5. Suspected or actual violations of the generation or issuance process; 6. CA certificate is compromised.	1. Sight revocation procedures cover the conditions described in the Control Step; 2. Sampled observations of incidents which meet revocation conditions are revoked.
41	The Auditor shall review that the CA has taken steps to verify the identity of the requestor of certificate revocation.	1. Sight the CA verification procedures; 2. Sampled observations of verification documents.

S/No	Control Steps	Checks
42	The Auditor shall review the certificate revocation information contain, but is not limited to the following: 1. Reason for revocation; 2. Revocation date/time. In addition, the Auditor shall review that the certificate revocation information is digitally signed and published by the CA.	1. Sampled observations of certification revocation information as described in the Control Step; 2. Sampled observations that the revocation information is digitally signed by the CA; 3. Sampled observations that the revocation information is published.
43	The Auditor shall review that the CA has informed the Subscriber of revoked certificates.	1. Sampled observations of communication that the CA has informed the Subscriber of revoked certificates within 1 hour.
44	The Auditor shall review that the CA has taken steps to ensure that the certificate revocation information is protected from unauthorized modifications.	1. Inquire the CA on protection mechanisms used to prevent unauthorized modifications of revocation information; 2. Sampled observations of the protection mechanisms.
45	The Auditor shall review that the CA do not re-activate revoked certificates.	1. Inquire the CA on measures taken to prevent the re-activation of revoked certificates; 2. Sampled observations of the measures.
Archival Process		
46	The Auditor shall review that all certificate suspension and revocation information, certificates, registration documents are archived for 7 years.	1. Sampled observations of archived information (one for each year).
47	The Auditor shall review that the CA tests the archival process for accuracy, security and accessibility for digital archives.	1. Sight test results; 2. Sight evidence that testing is performed at least yearly; 3. Sampled observations that negative testing has been rectified.
Audit Trails		
48	The Auditor shall review that the CA keeps audit trails of certificate registration, generation, issuance, renewal, suspension and revocation.	1. Inquire the CA on the audit trails kept; 2. Sampled observations of the audit trails.
49	The Auditor shall review the security mechanism the CA implements for the protection of audit trails.	1. Inquire the security mechanisms used to protect the audit trails; 2. Sampled observations of the security mechanisms.
50	The Auditor shall review that the CA conducts periodic reviews of the audit trails.	1. Sight audit review documents; 2. Sight evidence that audit trails are reviewed at least once every 2 days.
51	The Auditor shall review that the CA keeps audit trails for 12 months.	1. Sampled observations of audit trails (sampled for each month).

3. Key Management Controls

S/No	Control Steps	Checks
Generation		
52	The Auditor shall review that segregation of duties exists between personnel involved in system setup and maintenance and personnel involved in the key generation process. In addition, the Auditor shall also review that keys are stored under dual control.	1. Sight access control matrixes that conflicting roles are not present and dual control exists for key assignment; 2. Observation that system access controls are according to segregation of duties.
53	The Auditor shall review that separate key pairs exists for digital signature and encryption.	1. Observation of separate key pairs.
54	The Auditor shall review that the CA uses random key values in the generation of keys. The Auditor shall also review that the seed (input) used in the random generator is not static and not predictable.	1. Inquire the CA on how seeds are produced; 2. Sampled observations of seed generation.
55	The Auditor shall review that the CA provides reviews and approves the key generation system used by the Subscribers.	1. Sampled observations of approval of key generation system used by the Subscribers.
Distribution		
56	The Auditor shall review that the CA has prescribed procedures for transferring the keys from the key generation system to the storage device in a secure manner.	1. Inquire the CA on protection mechanism of transferring keys; 2. Sampled observations of the protection mechanism.
Storage		
57	The Auditor shall review the CA has provided Subscribers the necessary instructions and programs to safeguard and encrypt the Subscribers' private keys.	1. Sight instructions and programs to Subscribers.
58	The Auditor shall review that the CA stores its keys in tamper proof devices. In addition, the Auditor shall review that: 1. Access to the tamper proof devices is dual controlled by personnel not involved in the setup, maintenance and operations of the CA systems; 2. The CA documents and approves the change of key custodians; 3. Backup custodians to reduce key-man risks exist.	1. Observation of tamper proof devices; 2. Sampled observations of key custodian change documentation; 3. Sight access control matrixes for key custodians, backups and segregation of duties of custodians.
Usage		
59	The Auditor shall review that the CA implements dual control loading of the certificates. In addition, the Auditor shall review that the CA performs integrity checks prior to loading of the certificates.	1. Inquire the CA on procedures of dual control on loading of certificates; 2. Inquire the CA on integrity checks; 3. Sampled observations that integrity checks and dual control are implemented.
Backups		
60	The Auditor shall review that the CA private keys are backed up.	1. Observation of the backup private keys; 2. Sight evidence that the backup keys are subject to the same controls as the original keys.

S/No	Control Steps	Checks
61	The Auditor shall review that the CA stores its backup keys in a separate physical location as the original key.	1. Observation of separate physical location for backup keys.
Key Change		
62	The Auditor shall review that the CA change the CA and Subscriber keys periodically. In addition, the Auditor shall review that the CA has provided notice to: 1. The Subscribers' relying parties of new key pairs used to sign certificates; 2. The Subscriber or owner of changed key in a secured manner.	1. Sampled observations of key change documentation; 2. Sampled observations that the CA has provided notice to the Subscriber as defined in the Control Step.
63	The Auditor shall review that the CA has a key interlock procedure and implements the procedure during key change.	1. Sight the key interlock procedures; 2. Sampled observations that procedures were followed.
Destruction		
64	The Auditor shall review that the CA archives and securely stores the backup copies upon the termination of a CA signature private key.	1. Sampled observations of archives and backups.
Key Compromise		
65	The Auditor shall review that the CA has an escalation process in the event of suspected or actual key compromise. In addition, the Auditor should review that the Controller is informed within 24 hours of suspected or actual key compromise.	1. Inquire the CA of historical compromise; 2. Sample compromise events and sight for evidence that the CA has informed the Controller within 24 hours.
66	The Auditor shall review that the CA has revoked all affected Subscriber certificates in the event of CA certification private key compromise.	1. Inquire the CA of historical compromise; 2. Observation that affected certificates have been revoked.
67	The Auditor shall review that the CA has revoked all affected keys and certificates in the case of subscriber private key compromise.	1. Inquire the CA of historical compromise; 2. Observation that affected keys and certificates have been revoked.
Key Archival		
68	The Auditor shall review that the CA has archived: 1. All CA Public keys (permanently) 2. All Subscriber encryption keys.	1. Sampled observations of archives.
69	The Auditor shall review that the archives are protected from unauthorized modification.	1. Inquire the CA of the protection mechanisms; 2. Sampled observations of the protection mechanism having been implemented.

S/No	Control Steps	Checks
Cryptographic Engineering		
70	The Auditor shall review that the CA performs its cryptographic processes in a hardware cryptographic module that minimally conforms to: 1. FIPS 140-1 Security Level 3; 2. FIPS 140-2 Security Level 3. For Registration Authority (RA) operations away from the CA, the cryptographic module should minimally conform to: 1. FIPS 140-1 Security Level 2; 2. FIPS 140-2 Security Level 2.	1. Sight evidence that the cryptographic hardware used has the appropriate FIPS certification.
71	The Auditor shall review that the CA has communicated to its Subscribers that their cryptographic operation should conform minimally to: 1. FIPS 140-1 Security Level 1; 2. FIPS 140-2 Security Level 1.	1. Sampled observations of communication to Subscribers and that it contains the minimum requirement of FIPS compliance.
72	The Auditor shall review that the CA ensures: 1. Cryptographic keys and algorithms are sufficient to protect the cryptographic results; 2. Asymmetric cryptographic algorithms conform to the IEEE standard specifications.	1. Inquire the CA on the sufficiency testing of the cryptographic keys and algorithms; 2. Sight evidence that the asymmetric cryptographic algorithms used are IEEE compliant.

4. System and Operational Controls

S/No	Control Steps	Checks
73	The Auditor shall review that access control matrixes (physical and logical) are defined for all operating systems, network devices, applications and databases used in the CA operations exist. The access control matrixes should include, but are not limited to: 1. Personnel names; 2. Access granted; 3. Validity of access rights; 4. The next access control matrix review date. In addition, the Auditor shall review the application and currency of the access controls defined in the access control matrixes.	1. Sight access control matrix minimally covers the areas as defined in the Control Step; 2. Observation of system, network, application and database access controls are implemented in accordance to the access control matrix.
74	The Auditor shall review that the CA performs an assessment of the CA infrastructure components, which includes: 1. Operating system; 2. Network devices; 3. Security software (e.g. Intrusion Detection System and Anti-virus Software). A full assessment is required for new components and an incremental assessment is required for updates or modifications to the infrastructure.	1. Sight assessment report and follow-up actions. 2. Sampled observations that follow-up actions are implemented.
75	The Auditor shall review that the CA performs regular scans using tools of its systems and network devices to identify security vulnerabilities. The tools must be able to scan system and network vulnerabilities. In addition, the Auditor shall review that follow-up actions have been performed.	1. Sampled observations of scan results; 2. Sight evidence that scanning is performed at least once a week; 3. Sampled observations that follow-up actions are implemented.
76	The Auditor shall review that the CA has deployed Intrusion Detection System (IDS). In addition, the Auditor shall review that follow-up actions have been performed for potential intrusions.	1. Sampled observations of follow-up actions of detected intrusions; 2. Sight evidence that the IDS covers 100% of components of the CA infrastructure.
77	The Auditor shall review that the CA performs regular log review of the following (using the access control matrixes): 1. Unauthorized access and modifications to key system files and utilities; 2. Unauthorized access and modifications of Subscribers' data. The Auditor shall also review that follow-up actions has been performed for identified unauthorized access.	1. Observation of log review reports 2. Sampled observations that follow-up actions have been implemented.

S/No	Control Steps	Checks
Physical Security		
78	The Auditor shall review that: 1. The location of the CA system is not publicly identified; 2. Physical security systems are installed; 3. Inventory of access control cards are dual-controlled; 4. Loss of access control cards are reported and follow-up actions are performed; 5. Systems performing certification should be partitioned under lock and key; 6. Entry to the partition must be logged with timestamps; 7. Entry logs are reviewed: 8. Access to infrastructure components (power control, communication riders and cabling) is restricted to authorized personnel; 9. An approval process for temporal or bypass access exists; 10. An IDS exists.	1. Sampled observations that the CA carries out the items described in the Control Step; 2. Sight evidence that entry logs are reviewed daily.
General Security Controls		
79	The Auditor shall review that: 1. Systems performing certification functions are not used for general purposes (e.g. word processing, emailing, web surfing); 2. Strong password policies are implemented; 3. System administrators are trained; 4. CA application operators are trained; 5. Inactive lockouts are implemented (no longer than 10 minutes of inactivity before lockout); 6. Updated security patches are reviewed, tested, applied and implemented.	1. Sampled observations that the CA carries out the items described in the Control Step.
General Operational Controls		
80	The Auditor shall review that: 1. System administrators are trained; 2. CA application operators are trained.	1. Sampled observations of training records.
Change and Configuration Management		
81	The Auditor shall review that: 1. All changes are supported by change requests; 2. All change requests are approved before construction; 3. All source codes should be version-controlled; 4. There is an approved process of moving from development to production; 5. Segregation of duties exists for source code migration.	1. Sampled observations that the CA carries out the items described in the Control Step.
Network Security		
82	The Auditor shall review that: 1. Network access control exists to separate and isolate CA systems from the other systems; 2. Communications between CA systems should be secure and data should not be transmitted in the clear; 3. IDS is present and that the IDS monitors the CA systems.	1. Sampled observations that the CA carries out the items described in the Control Step.

S/No	Control Steps	Checks
Monitoring and Audit Trails		
83	The Auditor shall review that the CA has the following audit trails: 1. Application transactions: a. Registration; b. Certification; c. Publication; d. Suspension; and e. Revocation. 2. System log files: a. Security violations; b. Errors; c. Execution of privilege functions; d. Changes in access control and system configurations. In addition, the Auditor shall review that the: 1. audit trails are protected from unauthorized access; 2. and retained for a minimum period of 12 months.	1. Sampled observations of audit trails and that they cover the items described in the Control Step; 2. Inquire the CA on the protection mechanism of audit trails; 3. Sampled observations of the protection mechanism; 4. Sampled observations of audit trail retention (sample from each month).
84	The Auditor shall review that the CA performs regular reviews of the audit trails and follow-up actions are performed.	1. Observation of audit trail review reports; 2. Sampled observations that follow-up actions have been implemented.

5. Application Integration Controls

S/No	Control Steps	Checks
85	The Auditor shall review that the application toolkits provided by the CA to the user and developer community comply with the following: 1. The user shall be informed when a private key is being accessed; 2. The user shall be alerted if its private key is being used for a purpose that is not consistent with that defined as acceptable use by the issuer; 3. Mechanisms shall be available to check the integrity of the applications for unauthorised modifications, especially the integrity of signing and verification functions; 4. Application security risk assessment on the CA's software infrastructure should be conducted yearly to ensure that the CA's software that manages, issues and revokes certificates is developed to manage the risk identified; 5. The application should securely purge the private key temporarily stored for processing to minimise private key exposure; 6. The application shall verify the validity and authenticity of the certificate; 7. The verification process shall trace and verify all the components in the certification path; 8. For validity and authenticity verification, it shall be necessary to verify that: a. The certificate issuer's signature is valid; b. The certificate is valid (i.e. has not expired, been suspended or revoked); and c. The certificate extensions flagged as "critical" are being complied with.	1. Sight that each application toolkit provided by the CA minimally complied with the requirements as defined in the Control Step.

6. Compliance with ETA and ETR

S/No	Control Steps	Checks
Compliance with ETA		
86	The Auditor shall review that the CA has complied with the following paragraphs of the Third Schedule of the Electronic Transactions Act (ETA): • Sub-paragraph 10(1); • All of paragraph 12; • All of paragraph 13; • All of paragraph 14; • All of paragraph 16; • All of paragraph 17; • All of paragraph 18; • All of paragraph 19; • All of paragraph 20.	1. Inquire the CA on its compliance with the relevant provisions of the ETA as defined in the Control Step; 2. Sight evidence that the CA has complied with the relevant provisions of the ETA as defined in the Control Step.
Compliance with ETR		
87	The Auditor shall review that the CA has complied with the following regulations of the Electronic Transactions (Certification Authority) Regulations (ETR): • Sub-regulations 11(1) and 11(3); • All of regulation 12; • All of regulation 13; • All of regulation 14; • All of regulation 15; • Sub-regulations 16(2), 16(3), 16(4), 16(5), 16(6), 16(7), 16(9), 16(10) and 16(11); • Sub-regulations 17(2) and 17(3); • Sub-regulations 18(2), 18(3), 18(4), 18(6), 18(7), 18(8), 18(10) and 18(11); • All of regulation 19; • All of regulation 20 • Sub-regulations 21(1), 21(2), 21(3), 21(4), 21(5), 21(7), and 21(8); • All of regulation 22; • Sub-regulations 23(6), 23(7), 23(8), 23(9), and 23(10); • All of regulation 24; • All of regulation 25; • Sub-regulations 26(1) and 26(3); • All of regulation 27; • All of regulation 28; • Sub-regulation 29(1); • Sub-regulations 32(3) and 32(4).	1. Inquire the CA on its compliance with the relevant provisions of the ETR as defined in the Control Step; 2. Sight evidence that the CA has complied with the relevant provisions of the ETR as defined in the Control Step.