Triennial Compliance

Audit Requirements

March 16, 2010

Version v1.0.0

Revision History Table

Date	Version	Description	Author
10/15/09	0.0.1	First Released Version	CPWG Audit WG
11/18/09	0.0.2	WG Edits	CPWG Audit WG
11/20/09	0.0.3	WG edits	CPWG Audit WG
12/02/09	0.0.4	WG edits	CPWG Audit WG
01/21/10	0.0.5	CWPG review commendations	CPWG
03/16/10	1.0.0	CWPG Release Version	CPWG

Table of Contents

1.0 Introduction

This document represents the Audit Working Group (AWG) recommendations for annual compliance audit requirements. In developing the recommendations, the AWG considered compliance audit standards and existing federal matrices control statements that will be mandated for the Federal Common Policy Framework (FCPF) and Federal Bridge Certificate Authority (FBCA) certification annual audit.

The AWG acts under the authority of the Federal PKI Policy Authority (FPKIPA), and interacts with the Federal PKI Certificate Policy Working Group (CPWG). The AWG is charged with developing requirements for compliance audits. The AWG findings and recommendations are subject to the approval of the FPKIPA.

The AWG has reached the conclusion that a full and complete compliance audit of all mandatory criteria is required for the initial compliance audit. Subsequent compliance audits require review of previous year's discrepancies, evaluation of modifications and changes made over the last year, core criteria and triennial criteria.

The benefit to Federal agencies operating PKIs is an enhanced trust model and predictable annual budget allocation. Rather than a full compliance audit once every three-years and annual delta audits between, agencies will be able to amortize the budget cost over the three-years. Additionally, any changes and critical requirements will be audited for compliance annually. This change to the compliance audit requirements will establish a more trustworthy PKI.

2.0 Assessment Areas

The AWG has identified four (4) principal compliance audit areas that shall be performed annually:

1) Review of the previous compliance audit findings
2) Compliance audit of identified changes since the previous compliance audit
3) Compliance audit for FPKI Core Requirements, Appendix A - FPKI Annual Core Requirements
4) Compliance audit for FPKI Triennial Requirements, Appendix B - FPKI Triennial RFC Sections Requirements

The compliance auditor's assessment of findings shall be based on the pro forma FPKI Auditor Letter Of Compliance. The pro forma document can be found in Appendix C or at the FPKIPA web site.

The compliance audit report shall address the Compliance Audit Requirements (Cookbook).

The compliance auditor shall review previous compliance audit findings for associated changes and corrective actions. Similarly, the compliance auditor shall review changes to the system, policies, procedures, and personnel since the previous compliance audit.

These two activities shall be performed and the results assessed to determine the system's compliance.

The AWG performed an analysis of the FPKI assessment criteria (control) statements to determine the controls that present the greatest risk to a trusted relationship. The controls that represent the highest risk to an Entity's operation have been identified as "core" controls and shall be audited for compliance annually. The remaining controls are divided into three subsets or triennial controls. Each subset shall be audited for compliance once over the period of three (3) years. The combination of annual core controls and triennial controls over three (3) years shall be substituted for the previous requirement of a full compliance audit once every three (3) years and interim delta audits.

Each annual compliance audit shall be a complete and thorough assessment for the identified requirements. Components other than Certification Authorities (CAs) may be audited using a representative sample when necessary.

The FPKIPA has outlined a standard reporting structure for assessment reports. The FPKI Auditor Letter Of Compliance and Annotated Compliance Audit Cookbook are provided as templates to ensure a consistent evaluation of various audit communities. Additionally, these documents and other material can be located on the FPKIPA web site.

3.0 Criteria

The FPKI Compliance Audit requirements are separate and distinct from the certification and accreditation (C&A) requirements, however artifacts from the C&A may be useful to the compliance audit and vice-versa.

3.1 Initial Compliance Audit

When the Entity PKI is first established, an initial compliance audit shall be conducted. The initial compliance audit cannot evaluate all of the operational systems and procedures, as some of these systems have not yet produced auditable items.

3.2 First Year Compliance Audit

The Entity shall be responsible for a complete compliance audit within twelve months of the initial audit. All procedures and controls shall be audited for compliance and reported. The full audit includes the core requirements and all of the triennial requirements. The Entity may use Initial Compliance Audit findings as part of the full first year compliance audit. The first year full compliance audit shall constitute the baseline for the triennial audits.

3.3 Triennial Compliance Audit

The annual compliance audit consists of over 50 core controls statements that are critical to the trust relationship of an entity and the triennial requirements listed in section 2.0 above. The three triennial control tables contain the following (all section references assume RFC 3647 format):

- Year 1: CP Sections: 1, 4, 7, 9
- Year 2: CP Sections: 2, 3, 5, 8
- Year 3: CP Section: 6

The compliance auditor shall review previous compliance audit findings for associated changes and corrective actions.

The compliance auditor shall review all changes in policy, procedures, personnel, and system and technical aspects since the previous compliance audit. The compliance auditor shall perform an assessment of these changes as part of the compliance audit.

4.0 FPKI Compliance Audit Requirements

All newly established Entity CAs seeking cross-certification may submit an Initial Compliance Audit, but must complete a Full Compliance Audit during the first year. Existing Entity CAs must complete a Full Compliance Audit prior to cross-certification. Triennial requirements only apply to an Entity that has completed a full compliance audit and is currently cross certified with the FPKI.

There are specific requirements for the compliance audit letter submitted to the FPKIPA. The guidance can be found in Appendix C - FPKI Auditor Letter Of Compliance and Appendix D - The Annotated Compliance Audit Cookbook.

Appendix A - FPKI Annual Core Requirements

No.	RFC Section	Control Statement
1	RFC 1.5.3	The Certification Practices Statement must conform to the corresponding Certificate Policy. Entities must designate the person or organization that asserts that their CPS(s) conforms to their CP(s).
2	RFC 3.2.3	The Entity CAs and/or RAs shall record the information set forth below for issuance of each certificate: • The identity of the person performing the identification; • A signed declaration by that person that he or she verified the identity of the applicant as required using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law; • If in-person identity proofing is done, a unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s); • The date of the verification; and • A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law. *If an Applicant is unable to perform face-to-face registration (e.g., a network device), the applicant may be represented by a trusted person already issued a digital certificate by the Entity. The trusted person will present information sufficient for registration at the level of the certificate being requested, for both himself/herself and the applicant who the trusted person is representing.*
3	RFC 4.9.1	For Entity CAs, a certificate shall be revoked when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid. Entity CAs that implement certificate revocation shall, at a minimum, revoke certificates for the reason of key compromise upon receipt of an authenticated request from an appropriate entity.
4	RFC 4.9.8	CRLs shall be published within 4 hours of generation. Furthermore, each CRL shall be published no later than the time specified in the nextUpdate field of the previously issued CRL for same scope.
5	RFC 5.1	All CA equipment including CA cryptographic modules shall be protected from unauthorized access at all times.
6	RFC 5.1.2	The Entity CA equipment shall always be protected from unauthorized access. The security mechanisms shall be commensurate with the level of threat in the equipment environment.
7	RFC 5.1.2	Removable cryptographic modules, activation information used to access or enable cryptographic modules, and other sensitive CA equipment shall be placed in secure containers when not in use. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

No.	RFC Section	Control Statement
8	RFC: 5.1.2	The physical security requirements pertaining to CAs that issue Basic Assurance certificates are: • Ensure no unauthorized access to the hardware is permitted • Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers Comments: This requirement applies to Basic, but is different than the Medium requirement
9	RFC: 5.1.2	The physical security requirements pertaining to CAs that issue Basic Assurance certificates are: • Ensure no unauthorized access to the hardware is permitted • Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers In addition to those requirements, the following requirements shall apply to CAs that issue Medium, Medium Hardware, or High assurance certificates: • Ensure manual or electronic monitoring for unauthorized intrusion at all times • Ensure an access log is maintained and inspected periodically • Require two person physical access control to both the cryptographic module and computer system *Practice Note: Multiparty physical access control to CA equipment can be achieved by any combination of two or more trusted roles (see Section 5.2.2) as long as the tasks being conducted are segregated in accordance with the requirements and duties defined for each trusted role. As an example, an Auditor and an Operator might access the site housing the CA equipment to perform a tape backup, but only the Operator may perform the tape backup.*
10	RFC: 5.1.2	A security check of the facility housing the Entity CA equipment shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following: • The equipment is in a state appropriate to the current mode of operation (*e.g., that cryptographic modules are in place when “open”, and secured when “closed”*); • Any security containers are properly secured; • Physical security systems (e.g., door locks, vent covers) are functioning properly; and • The area is secured against unauthorized access.
11	RFC: 5.1.2	A person or group of persons shall be made explicitly responsible for making [security] checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.
12	RFC 5.1.2	RA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The RA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the RA equipment environment.

No.	RFC Section	Control Statement
13	RFC 5.1.2	Physical access control requirements for CSS equipment (if implemented), shall meet the CA physical access requirements specified in 5.1.2.1.
14	RFC 5.1.6	Entity CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). Entity CA media shall be stored so as to protect it from unauthorized physical access.
15	RFC 5.1.7	Sensitive media and documentation that are no longer needed for operations shall be destroyed in a secure manner. For example, sensitive paper documentation shall be shredded, burned, or otherwise rendered unrecoverable.
16	RFC: 5.1.8	For Entity CAs, full system backups sufficient to recover from system failure shall be made on a periodic schedule. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy shall be stored at an off-site location separate from the Entity CA equipment. Only the latest full backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational Entity CA.
17	RFC: 5.2.2	Two or more persons are required per task for the following tasks: • CA key generation; • CA signing key activation; • CA private key backup. Where multiparty control for logical access is required, at least one of the participants shall be an Administrator. All participants must serve in a trusted role as defined in Section 5.2.1. Multiparty control for logical access shall not be achieved using personnel that serve in the Auditor Trusted Role. Physical access to the CAs does not constitute a task as defined in this section. Therefore, two-person physical access control may be attained as required in Section 5.1.2.1.
18	RFC: 5.2.4	Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role; however, no one individual shall assume both the Officer and Administrator roles. This may be enforced procedurally. No individual shall be assigned more than one identity. Comments: This requirement applies to Basic, but is different than the Medium requirement
19	RFC: 5.2.4	Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may only assume one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. The CA and RA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer role, assume both the Administrator and Auditor roles, and assume both the Auditor and Officer roles. No individual shall have more than one identity.
20	RFC: 5.2.4	Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume only one of the Officer, Administrator and Auditor roles. Individuals designated as Officer or Administrator may also assume the Operator role. An auditor may not assume any other role. The CA and RA software and hardware shall identify and authenticate its users and shall enforce these roles. No individual shall have more than one identity. Comments: This requirement applies to High, but not to Medium HW

No.	RFC Section	Control Statement
21	RFC 5.3.1	All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity.
22	RFC 5.3.1	For Federal Agency PKIs, regardless of the assurance level, all trusted roles are required to be held by U.S. citizens.
23	RFC 5.3.2	Entity CA personnel shall, at a minimum, pass a background investigation covering the following areas: • Employment; • Education; • Place of residence; • Law Enforcement; and • References. The period of investigation must cover at least the last five years for each area, excepting the residence check which must cover at least the last three years. Regardless of the date of award, the highest educational degree shall be verified. Adjudication of the background investigation shall be performed by a competent adjudication authority using a process consistent with Executive Order 12968 August 1995, or equivalent.
24	RFC 5.3.3	All personnel performing duties with respect to the operation of the Entity CA shall receive comprehensive training in all operational duties they are expected to perform, including disaster recovery and business continuity procedures.
25	RFC 5.3.3	Personnel performing duties with respect to the operation of the Entity CA shall receive comprehensive training, or demonstrate competence, in the following areas: • CA/RA security principles and mechanisms; • All PKI software versions in use on the CA system. Documentation shall be maintained identifying all personnel who received training and the level of training completed. Where competence was demonstrated in lieu of training, supporting documentation shall be maintained.
26	RFC 5.3.4	Individuals responsible for PKI roles shall be aware of changes in the Entity CA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Documentation shall be maintained identifying all personnel who received training and the level of training completed.
27	RFC 5.3.7	Contractor personnel employed to perform functions pertaining to an Entity CA shall meet the personnel requirements set forth in the Entity CP.
28	RFC 5.3.8	For Entity CAs, documentation sufficient to define duties and procedures for each trusted role shall be provided to the personnel filling that role.
29	RFC 5.4	Audit log files shall be generated for all events relating to the security of the Entity CAs. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.
39	RFC 5.4.1	A message from any source received by the Entity CA requesting an action related to the operational state of the CA is an auditable event. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event): • The type of event, • The date and time the event occurred, • A success or failure indicator, where appropriate, • The identity of the entity and/or operator (of the Entity CA) that caused the event.
31	RFC 5.4.1	All security auditing capabilities of the Entity CA operating system and CA applications shall be enabled. Where events cannot be automatically recorded, the CA shall implement manual procedures to satisfy this requirement.

No.	RFC Section	Control Statement
32	RFC: 5.4.2	Audit logs shall be reviewed as required for cause. *Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs.* Actions taken as a result of these reviews shall be documented. Comments: This requirement applies to Basic, but is different than the Medium requirement
33	RFC: 5.4.2	Audit logs shall be reviewed at least once every two months *Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs.* Actions taken as a result of these reviews shall be documented. A statistically significant set of security audit data generated by Entity CAs since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity.
34	RFC: 5.4.2	Audit logs shall be reviewed at least once per month Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented. A statistically significant set of security audit data generated by Entity CAs since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. Comment: This requirement applies to High, but not to Medium HW
35	RFC 5.4.3	The individual who removes audit logs from the Entity CA system shall be an official different from the individuals who, in combination, command the Entity CA signature key.
36	RFC 5.4.4	Entity CA system configuration and procedures must be implemented together to ensure that: • Only personnel assigned to trusted roles have read access to the logs; • Only authorized people may archive audit logs; and, • Audit logs are not modified.
37	RFC 5.4.4	The entity performing audit log archive need not have modify access, but procedures must be implemented to protect archived data from destruction prior to the end of the audit log retention period (note that deletion requires modification access).
38	RFC 5.4.5	Audit logs and audit summaries shall be backed up at least monthly. A copy of the audit log shall be sent off-site on a monthly basis.
39	RFC 5.4.6	Automated audit processes shall be invoked at system (or application startup), and cease only at system (or application) shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the Entity Operational Authority Administrator shall determine whether to suspend Entity CA operation until the problem is remedied.

No.	RFC Section	Control Statement
40	RFC 5.4.8	For Entity CAs, personnel shall perform routine assessments for evidence of malicious activity. *Practice Note: The security audit data should be reviewed by the security auditor for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Security auditors should check for continuity of the security audit data.*

No.	RFC Section	Control Statement
41	RFC: 5.5.1	At a minimum, the following data shall be recorded for archive:

Data To Be Archived	Basic
CA accreditation (if applicable)	X
Certificate Policy	X
Certification Practice Statement	X
Contractual obligations	X
Other agreements concerning operations of the CA	X
System and equipment configuration	X
Modifications and updates to system or configuration	X
Certificate requests	X
Revocation requests	X
Subscriber identity Authentication data as per Section 3.2.3	X
Documentation of receipt and acceptance of certificates	X
Subscriber Agreements	X
Documentation of receipt of tokens	X
All certificates issued or published	X
Record of CA Re-key	X
All CRLs issued and/or published	X
Other data or applications to verify archive contents	X
Compliance Auditor reports	X
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	X
Any attempt to delete or modify the Audit logs	X
Whenever the CA generates a key (Not mandatory for single session or one-time use symmetric keys)	X
All access to certificate subject private keys retained within the CA for key recovery purposes	X
All changes to the trusted public keys, including additions and deletions	X
The export of private and secret keys (keys used for a single session or message are excluded)	X
The approval or rejection of a certificate status change request	X

<table>
<tr><th>No.</th><th>RFC Section</th><th>Control Statement</th></tr>
<tr><td>42</td><td>RFC:
5.5.1</td><td>At a minimum, the following data shall be recorded for archive:
<table>
<tr><th>Data To Be Archived</th><th>Medium</th></tr>
<tr><td>CA accreditation (if applicable)</td><td>X</td></tr>
<tr><td>Certificate Policy</td><td>X</td></tr>
<tr><td>Certification Practice Statement</td><td>X</td></tr>
<tr><td>Contractual obligations</td><td>X</td></tr>
<tr><td>Other agreements concerning operations of the CA</td><td>X</td></tr>
<tr><td>System and equipment configuration</td><td>X</td></tr>
<tr><td>Modifications and updates to system or configuration</td><td>X</td></tr>
<tr><td>Certificate requests</td><td>X</td></tr>
<tr><td>Revocation requests</td><td>X</td></tr>
<tr><td>Subscriber identity Authentication data as per Section 3.2.3</td><td>X</td></tr>
<tr><td>Documentation of receipt and acceptance of certificates</td><td>X</td></tr>
<tr><td>Subscriber Agreements</td><td>X</td></tr>
<tr><td>Documentation of receipt of tokens</td><td>X</td></tr>
<tr><td>All certificates issued or published</td><td>X</td></tr>
<tr><td>Record of CA Re-key</td><td>X</td></tr>
<tr><td>All CRLs issued and/or published</td><td>X</td></tr>
<tr><td>Other data or applications to verify archive contents</td><td>X</td></tr>
<tr><td>Compliance Auditor reports</td><td>X</td></tr>
<tr><td>Any changes to the Audit parameters, e.g., audit frequency, type of event audited</td><td>X</td></tr>
<tr><td>Any attempt to delete or modify the Audit logs</td><td>X</td></tr>
<tr><td>Whenever the CA generates a key (Not mandatory for single session or one-time use symmetric keys)</td><td>X</td></tr>
<tr><td>All access to certificate subject private keys retained within the CA for key recovery purposes</td><td>X</td></tr>
<tr><td>All changes to the trusted public keys, including additions and deletions</td><td>X</td></tr>
<tr><td>The export of private and secret keys (keys used for a single session or message are excluded)</td><td>X</td></tr>
<tr><td>The approval or rejection of a certificate status change request</td><td>X</td></tr>
</table>
</td></tr>
</table>

No.	RFC Section	Control Statement
43	RFC 5.7.3	If the Entity CA signature keys are compromised or lost (such that compromise is possible even though not certain): • [All affiliated] entities shall be notified so that entities may issue CRLs revoking any cross-certificates issued to the compromised CA; • A new Entity CA key pair shall be generated by the Entity CA in accordance with procedures set forth in the Entity CPS; and • New Entity CA certificates shall be issued to Entities also in accordance with the Entity CPS. The Entity CA governing body shall also investigate and report what caused the compromise or loss, and what measures have been taken to preclude recurrence.
44	RFC 5.7.3	If the CA distributes its key in a self-signed certificate, the new self-signed certificate shall be distributed as specified in Section 6.1.4.
45	RFC 6.1.1	CA key pair generation must create a verifiable audit trail that the security requirements for procedures were followed. For all levels of assurance, the documentation of the procedure must be detailed enough to show that appropriate role separation was used. *Practice Note: If the audit trail identifies and documents any failures or anomalies in the key generation process, along with the corrective action taken, the key generation process need not be restarted but may continue.*
46	RFC: 6.1.1	*[At all levels] CA key pair generation must create a verifiable audit trail that the security requirements for procedures were followed. For all levels of assurance, the documentation of the procedure must be detailed enough to show that appropriate role separation was used.* [An] independent third party shall validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation. Comments: Not Basic
47	RFC 6.1.2	When CAs or RAs generate keys on behalf of the Subscriber, then the private key must be delivered securely to the Subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements must be met: • Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the private key to the Subscriber. • The private key must be protected from activation, compromise, or modification during the delivery process. • The Subscriber shall acknowledge receipt of the private key(s). • Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers. o For hardware modules, accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it. o For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel. The Entity CA must maintain a record of the subscriber acknowledgement of receipt of the token.

No.	RFC Section	Control Statement
48	RFC 6.2.9	Cryptographic modules that have been activated shall not be available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS. CA Hardware cryptographic modules shall be removed and stored in a secure container when not in use.
49	RFC 6.5.1	The Entity CA and its ancillary parts shall include the following functionality: • authenticate the identity of users before permitting access to the system or applications; • manage privileges of users to limit users to their assigned roles; • generate and archive audit records for all transactions; (see Section 5.4) • enforce domain integrity boundaries for security critical processes; and • support recovery from key or system failure. *These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards*
50	RFC 6.5.1	For Certificate Status Servers, the computer security functions listed below are required: • authenticate the identity of users before permitting access to the system or applications; • manage privileges of users to limit users to their assigned roles; • enforce domain integrity boundaries for security critical processes; and • support recovery from key or system failure.
51	RFC: 6.6.1	The System Development Controls for the Entity CAs are as follows: • Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment. Hardware and software shall be scanned for malicious code on first use and periodically thereafter.
52	RFC 6.6.2	The configuration of the Entity CA system as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the Entity CA software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of the Entity CA system. The Entity CA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use.
53	RFC 6.7	Entity CAs, RAs, directories and certificate status servers shall employ appropriate network security controls. Networking equipment shall turn off unused network ports and services. Any network software present shall be necessary to the functioning of the equipment.
54	RFC 8.1	The Entity Principal CAs and RAs and their subordinate CAs and RAs shall be subject to a periodic compliance audit at least once per year for High, Medium Hardware, and Medium Assurance, and at least once every two years for Basic Assurance. Where a status server is specified in certificates issued by a CA, the status server shall be subject to the same periodic compliance audit requirements as the corresponding CA. For example, if an OCSP server is specified in the authority information access extension in certificates issued by a CA, that server must be reviewed as part of that CA's compliance audit.
55	RFC 8.2	The auditor must demonstrate competence in the field of compliance audits. At the time of the audit, the Entity CA compliance auditor must be thoroughly familiar with the requirements which Entities impose on the issuance and management of their certificates. The compliance auditor must perform such compliance audits as a regular ongoing business activity.

No.	RFC Section	Control Statement
56	RFC 8.4	The purpose of a compliance audit of an Entity PKI shall be to verify that an entity subject to the requirements of an Entity CP is complying with the requirements of those documents, as well as any MOAs between the Entity PKI and any other PKI.
57	RFC 8.5	When the Entity compliance auditor finds a discrepancy between how the Entity CA is designed or is being operated or maintained, and the requirements of the Entity CP, any applicable MOAs, or the applicable CPS, the following actions shall be performed: • The compliance auditor shall document the discrepancy; • The compliance auditor shall notify the responsible party promptly; • The Entity PKI shall determine what further notifications or actions are necessary to meet the requirements of the Entity CP, CPS, and any relevant MOA provisions. The Entity PKI shall proceed to make such notifications and take such actions without delay.
58	RFC 5.4.1	Refer to table below for Types of Events Recorded. Review Level of Assurance for rquirement.

FBCA 5.4.1 – Types of Events Recorded

Comments: Basic

	Auditable Event		Basic
	SECURITY AUDIT		
1	Any changes to the Audit parameters, e.g., audit frequency, type of event audited		**X**
2	Any attempt to delete or modify the Audit logs		**X**
3	Obtaining a third-party time-stamp		**X**
	IDENTIFICATION AND AUTHENTICATION		
4	Successful and unsuccessful attempts to assume a role		**X**
5	The value of *maximum authentication attempts* is changed		**X**
6	The number of unsuccessful authentication attempts exceeds the *maximum authentication attempts* during user login		**X**
7	An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts		**X**
8	An Administrator changes the type of authenticator, e.g., from password to biometrics		**X**
	LOCAL DATA ENTRY		
9	All security-relevant data that is entered in the system		**X**
	REMOTE DATA ENTRY		
10	All security-relevant messages that are received by the system		**X**
	DATA EXPORT AND OUTPUT		
11	All successful and unsuccessful requests for confidential and security-relevant information		**X**
	KEY GENERATION		
12	Whenever the Entity CA generates a key. (Not mandatory for single session or one-time use symmetric keys)		**X**
	PRIVATE KEY LOAD AND STORAGE		
13	The loading of Component private keys		**X**
14	All access to certificate subject private keys retained within the Entity CA for key recovery purposes		**X**
	TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE		
15	All changes to the trusted public keys, including additions and deletions		**X**
	SECRET KEY STORAGE		
16	The manual entry of secret keys used for authentication		
	PRIVATE AND SECRET KEY EXPORT		

	Auditable Event		**Basic**
17	The export of private and secret keys (keys used for a single session or message are excluded)		**X**
	CERTIFICATE REGISTRATION		
18	All certificate requests		**X**
	CERTIFICATE REVOCATION		
19	All certificate revocation requests		**X**
	CERTIFICATE STATUS CHANGE APPROVAL		
20	The approval or rejection of a certificate status change request		**X**
	ENTITY CA CONFIGURATION		
21	Any security-relevant changes to the configuration of the Entity CA		**X**
	ACCOUNT ADMINISTRATION		
22	Roles and users are added or deleted		**X**
23	The access control privileges of a user account or a role are modified		**X**
	CERTIFICATE PROFILE MANAGEMENT		
24	All changes to the certificate profile		**X**
	REVOCATION PROFILE MANAGEMENT		
25	All changes to the revocation profile		**X**
	CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT		
26	All changes to the certificate revocation list profile		**X**
	MISCELLANEOUS		
27	*Appointment of an individual to a Trusted Role*		**X**
28	*Designation of personnel for multiparty control*		
29	*Installation of the Operating System*		**X**
30	*Installation of the Entity CA*		**X**
31	*Installing hardware cryptographic modules*		
32	*Removing hardware cryptographic modules*		
33	*Destruction of cryptographic modules*		**X**
34	*System Startup*		**X**
35	*Logon Attempts to Entity CA Apps*		**X**
36	*Receipt of Hardware / Software*		
37	*Attempts to set passwords*		**X**
38	*Attempts to modify passwords*		**X**
39	*Backing up Entity CA internal database*		**X**
40	*Restoring Agency CA internal database*		**X**
41	*File manipulation (e.g., creation, renaming, moving)*		
42	*Posting of any material to a repository*		
43	*Access to Entity CA internal database*		
44	*All certificate compromise notification requests*		**X**
45	*Loading tokens with certificates*		
46	*Shipment of Tokens*		
47	*Zeroizing tokens*		**X**
48	*Rekey of the Entity CA*		**X**
	Configuration changes to the CA server involving:		
49	*Hardware*		**X**
50	*Software*		**X**
51	*Operating System*		**X**
52	*Patches*		**X**
53	*Security Profiles*		
	PHYSICAL ACCESS / SITE SECURITY		
54	*Personnel Access to room housing Entity CA*		
55	*Access to the Entity CA server*		

	Auditable Event		Basic
56	*Known or suspected violations of physical security*		**X**
	ANOMALIES		
57	*Software Error conditions*		**X**
58	*Software check integrity failures*		**X**
59	*Receipt of improper messages*		
60	*Misrouted messages*		
61	*Network attacks (suspected or confirmed)*		**X**
62	*Equipment failure*		**X**
63	*Electrical power outages*		
64	*Uninterruptible Power Supply (UPS) failure*		
65	*Obvious and significant network service or access failures*		
66	*Violations of Certificate Policy*		**X**
67	*Violations of Certification Practice Statement*		**X**
68	*Resetting Operating System clock*		**X**

Comments: Medium, Medium CBP, Medium Hardware, Medium Hardware CBP and High.

	Auditable Event		FBCA
	SECURITY AUDIT		
1	Any changes to the Audit parameters, e.g., audit frequency, type of event audited		**X**
2	Any attempt to delete or modify the Audit logs		**X**
3	Obtaining a third-party time-stamp		**X**
	IDENTIFICATION AND AUTHENTICATION		
4	Successful and unsuccessful attempts to assume a role		**X**
5	The value of *maximum authentication attempts* is changed		**X**
6	The number of unsuccessful authentication attempts exceeds the *maximum authentication attempts* during user login		**X**
7	An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts		**X**
8	An Administrator changes the type of authenticator, e.g., from password to biometrics		**X**
	LOCAL DATA ENTRY		
9	All security-relevant data that is entered in the system		**X**
	REMOTE DATA ENTRY		
10	All security-relevant messages that are received by the system		**X**
	DATA EXPORT AND OUTPUT		
11	All successful and unsuccessful requests for confidential and security-relevant information		**X**
	KEY GENERATION		
12	Whenever the Entity CA generates a key. (Not mandatory for single session or one-time use symmetric keys)		**X**
	PRIVATE KEY LOAD AND STORAGE		
13	The loading of Component private keys		**X**
14	All access to certificate subject private keys retained within the Entity CA for key recovery purposes		**X**
	TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE		
15	All changes to the trusted public keys, including additions and deletions		**X**
	SECRET KEY STORAGE		
16	The manual entry of secret keys used for authentication		**X**
	PRIVATE AND SECRET KEY EXPORT		
17	The export of private and secret keys (keys used for a single session or message are		**X**

	Auditable Event		FBCA
	excluded)		
	CERTIFICATE REGISTRATION		
18	All certificate requests		**X**
	CERTIFICATE REVOCATION		
19	All certificate revocation requests		**X**
	CERTIFICATE STATUS CHANGE APPROVAL		
20	The approval or rejection of a certificate status change request		**X**
	FBCA OR ENTITY CA CONFIGURATION		
21	Any security-relevant changes to the configuration of the FBCA or Entity CA		**X**
	ACCOUNT ADMINISTRATION		
22	Roles and users are added or deleted		**X**
23	The access control privileges of a user account or a role are modified		**X**
	CERTIFICATE PROFILE MANAGEMENT		
24	All changes to the certificate profile		**X**
	REVOCATION PROFILE MANAGEMENT		
25	All changes to the revocation profile		**X**
	CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT		
26	All changes to the certificate revocation list profile		**X**
	MISCELLANEOUS		
27	*Appointment of an individual to a Trusted Role*		**X**
28	*Designation of personnel for multiparty control*		**X**
29	*Installation of the Operating System*		**X**
30	*Installation of the FBCA or Entity CA*		**X**
31	*Installing hardware cryptographic modules*		**X**
32	*Removing hardware cryptographic modules*		**X**
33	*Destruction of cryptographic modules*		**X**
34	*System Startup*		**X**
35	*Logon Attempts to FBCA or Entity CA Apps*		**X**
36	*Receipt of Hardware / Software*		**X**
37	*Attempts to set passwords*		**X**
38	*Attempts to modify passwords*		**X**
39	*Backing up FBCA or Entity CA internal database*		**X**
40	*Restoring FBCA or Agency CA internal database*		**X**
41	*File manipulation (e.g., creation, renaming, moving)*		**X**
42	*Posting of any material to a repository*		**X**
43	*Access to FBCA or Entity CA internal database*		**X**
44	*All certificate compromise notification requests*		**X**
45	*Loading tokens with certificates*		**X**
46	*Shipment of Tokens*		**X**
47	*Zeroizing tokens*		**X**
48	*Rekey of the FBCA or Entity CA*		**X**
	Configuration changes to the CA server involving:		
49	*Hardware*		**X**
50	*Software*		**X**
51	*Operating System*		**X**
52	*Patches*		**X**
53	*Security Profiles*		**X**
	PHYSICAL ACCESS / SITE SECURITY		
54	*Personnel Access to room housing FBCA or Entity CA*		**X**
55	*Access to the FBCA or Entity CA server*		**X**
56	*Known or suspected violations of physical security*		**X**

	Auditable Event		FBCA
	ANOMALIES		
57	*Software Error conditions*		**X**
58	*Software check integrity failures*		**X**
59	*Receipt of improper messages*		**X**
60	*Misrouted messages*		**X**
61	*Network attacks (suspected or confirmed)*		**X**
62	*Equipment failure*		**X**
63	*Electrical power outages*		**X**
64	*Uninterruptible Power Supply (UPS) failure*		**X**
65	*Obvious and significant network service or access failures*		**X**
66	*Violations of Certificate Policy*		**X**
67	*Violations of Certification Practice Statement*		**X**
68	*Resetting Operating System clock*		**X**

Appendix B - FPKI Triennial RFC Sections Requirements

Non-core Entity CP/CPS assertions are divided into three categories. These three subsets cover all Entity assertions by RFC section number. The three triennial requirements consist of the following RFC section division:

Year	RFC Sections	Description
1	1, 4, 7 and 9	
2	2, 3, 5 and 8	
3	6	

The cycle will resume at Year 1 on the fourth, seventh, etc. following years.

Appendix C - FPKI Auditor Letter Of Compliance

Compliance Audit Requirements

October 28, 2009

These requirements apply to all cross-certified entities under the FBCA CP or through the Common Policy.

In order to evaluate a compliance audit, the following background information is required.

- Identity of the Auditor and the individuals performing the audit;
- Competence of the Auditor to perform audits;
- Experience of the individuals performing the audit in auditing PKI systems;
- Relationship of the Auditor to the entity that owns the PKI being audited. This relationship must clearly demonstrate the independence of the auditor from the entity operating or managing the PKI.

The following information regarding the audit itself is required.

- The date the audit was performed.
- Whether a particular methodology was used, and if so, what methodology.
- Which documents were reviewed as a part of the audit, including document dates and version numbers.

In addition to this background, the entity should ensure that, as part of the audit, an audit summary is prepared, signed by the auditor, reporting on the following elements after conducting the compliance audit:

- State that the operations of the entity PKI's Principal CA were evaluated for conformance to the requirements of its CPS.
- Report the findings of the evaluation of operational conformance to the Principal CA CPS.
- State that the entity PKI's Principal CA CPS was evaluated for conformance to the entity PKI's CP.
- Report the findings of the evaluation of the Principal CA CPS conformance to the entity PKI CP.
- For PKIs with multiple CAs, state whether audit reports showing compliance were on file for any additional CA components of the entity PKI
- State that the operations of the Entity PKI's Principal CA were evaluated for conformance to the requirements of all cross-certification MOAs executed by

the Entity PKI with other entities. If there are no MOAs or other comparable agreements, this requirement does not apply.

- Report the findings of the evaluation of the Principal CA CPS conformance to the requirements of all cross-certification MOAs executed by the Entity PKI. If there are no MOAs or other comparable agreements, this requirement does not apply.

Auditing New CAs

Where the Entity PKI being audited is new and some procedures have only been performed in test environments, the report must include the following:

1. State which procedures have been performed using the operational system and could be fully evaluated for conformance to the requirements of the entity PKI CPS;
2. Report the findings of the evaluation in "1." above;
3. State which procedures have not been performed on the operational system and were evaluated for conformance to the requirements of the entity PKI CPS, but only with respect to training and procedures;
4. Report the findings of the evaluation in "3." above;
5. State that the entity PKI's CPS was evaluated for conformance to the supported certificate policies;
6. Report the findings of the evaluation in "5." above.

Note: These requirements are separate and distinct from the certification and accreditation requirements imposed by the Designated Approving Authority (DAA).

Since the FBCA/Common Policy CPs are neutral as to audit methodology, and do not prefer one methodology over another, any audit approach is acceptable provided that these points are addressed.

At the present time, a default WebTrust for CA audit will not satisfy the requirements set forth above. To meet FBCA/Common Policy requirements, the management assertions of the entity being audited would need to include the substance of the following assertions:

1. The Entity-CPS conforms to the requirements of the Entity-CP
2. The Entity-CA is operated in conformance with the requirements of the Entity-CPS;
3. The Entity-CA has maintained effective controls to provide reasonable assurance that:
    - Procedures defined in Section 1 of the Entity-CPS are in place and operational.
    - Procedures defined in Section 2 of the Entity-CPS are in place and operational.

- Procedures defined in Section 3 of the Entity-CPS are in place and operational.
- Procedures defined in Section 4 of the Entity-CPS are in place and operational.
- Procedures defined in Section 5 of the Entity-CPS are in place and operational.
- Procedures defined in Section 6 of the Entity-CPS are in place and operational.
- Procedures defined in Section 7 of the Entity-CPS are in place and operational.
- Procedures defined in Section 8 of the Entity-CPS are in place and operational.
- Procedures defined in Section 9 subsections 9.4.4 and 9.6.3 are in place and operational.

4. The Entity-CA is operated in conformance with the requirements of all cross-certification MOAs executed by the Entity-CA. If there are no MOAs or other comparable agreements, this requirement does not apply.

Note: *The FBCA/Common Policy does not require and will not consider any statements with respect to the entity PKI's suitability for cross certification with the FBCA/Common Policy or conformance to the FBCA/Common Policy certificate policies. Such a determination is exclusively the purview of the FPKIPA and its working groups.*

Appendix D - The Annotated Compliance Audit Cookbook

(Based on 10-20-2009 guidance)

Audit Guidance	Commentary
Identity of the Auditor and the individuals performing the audit	Who did the audit? Many of the big auditing concerns are partnerships or corporations that assert that the corporate entity performed the audit. While that's true in one sense, the CPWG wants the individual auditors identified – see the following regarding competence and experience.
Competence of the Auditor to perform audits	Individuals have competence, partnerships and corporations do not. The CPWG is looking for the individual auditor's credentials here.
Experience of the individuals performing the audit in auditing PKI systems	It's not enough to be a good auditor, the auditor should have some relevant IT or IT Security experience – or have audited a number of CAs.
Relationship of the Auditor to the entity that owns the PKI being audited. This relationship must clearly demonstrate the independence of the auditor from the entity operating or managing the PKI.	The Auditor needs to be independent and not conflicted.
The date the audit was performed.	As a reality check, if the audit is performed in May of 2009, the date on the CP and CPS should not be July of 2009.
Whether a particular methodology was used, and if so, what methodology.	At the present time, the CPWG is methodology neutral.
Which documents were reviewed as a part of the audit, including document dates and version numbers.	At a MINIMUM the CP and CPS should be identified here – as well as any other document relied upon in conducting the audit.
an audit summary is prepared, signed by the auditor	Yes, the report needs to be signed – wet signature or electronic. As a practical matter, it's good practice to include contact information for the auditor (e-mail and telephone number) in case further clarification is needed.
State that the operations of the entity PKI's Principal CA were evaluated for conformance to the requirements of its CPS.	This is where most audits fail. As discussed in the guidance, a plain vanilla WebTrust for CA audit will not meet this requirement, as the suggested controls in the WebTrust methodology do not necessarily capture all of the CPS requirements.
Report the findings of the evaluation of operational conformance to the Principal CA CPS.	If the operations are not 100% in accordance with the CPS, the CPWG will want details on what's deficient.

State that the entity PKI's Principal CA CPS was evaluated for conformance to the entity PKI's CP.	This is the second most frequent area where audits fail. Most methodologies do not compare the requirements of the CPS to the CP. If the CPS omits requirements imposed by the CP, the CPWG would like to know about it.
Report the findings of the evaluation of the Principal CA CPS conformance to the entity PKI CP.	Again, if the CPS is not 100% in accordance with the CP, the CPWG will want details on what's deficient.
For PKIs with multiple CAs, state whether audit reports showing compliance were on file for any additional CA components of the entity PKI	When there are multiple CAs, there should be (passing) compliance audits on file for the other CAs.
State that the operations of the Entity PKI's Principal CA were evaluated for conformance to the requirements of all current cross-certification MOAs executed by the Entity PKI with other entities.	In many instances, the MOA imposes requirements on the CA. These should be examined.
Report the findings of the evaluation of the Principal CA CPS conformance to the requirements of all current cross-certification MOAs executed by the Entity PKI.	If there is anything other than 100% compliance with MOA imposed requirements, the CPWG would like to know about it.