



Federal Public Key Infrastructure (FPKI) Compliance Audit Requirements

July 10, 2015

Version v2.0.1

REVISION HISTORY TABLE

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
4/10/2012	2.0.0	CPWG Release Version, updated to consolidate all audit requirements	CPWG
7/10/2015	2.0.1	Internal update to clarify Bridge & Day Zero and Package submission to ensure entire PKI is audited	FPKIPA Support

TABLE OF CONTENTS

1 INTRODUCTION.....1

2 AUDIT REQUIREMENTS2

 2.1 DAY ZERO COMPLIANCE AUDIT..... 2

 2.2 FULL COMPLIANCE AUDIT 2

 2.3 TRIENNIAL COMPLIANCE AUDIT 3

3 AUDIT REPORTING PROCESS4

APPENDIX A FPKI ANNUAL CORE REQUIREMENTS6

APPENDIX B AUDITOR LETTER OF COMPLIANCE TEMPLATE19

APPENDIX C AUDITOR COMPLIANCE SUMMARY TEMPLATE.....22

APPENDIX D THE ANNOTATED COMPLIANCE AUDIT COOKBOOK24

1 INTRODUCTION

Independent compliance audits are the mechanism used by the Federal Public Key Infrastructure Policy Authority (FPKIPA) to ensure that participating Public Key Infrastructure (PKIs), also called “Entities”, are operated in conformance with the requirements identified in the appropriate Certificate Policy (CP). Participating PKIs include all members of the Federal PKI (FPKI): Shared Service Providers (SSPs) operating under the Federal Common Policy CP, cross-certified PKIs operating under their own CPs that may be Federal Agency PKIs, other government PKIs, Commercial PKIs, and Bridges representing other communities of interest.

The FPKI Compliance Audit requirements are separate and distinct from the Federal authorization and accreditation (A&A) requirements levied on US Government agencies and SSPs. However, artifacts from the A&A may be useful to the compliance audit and vice-versa.

This document provides detailed guidance regarding requirements for performing and reporting annual compliance audits. It includes guidance for performing audits based on a three-year cycle, with an initial compliance audit that includes a full audit of all mandatory criteria and subsequent compliance audits that require a review of the previous year’s discrepancies, evaluation of modifications and changes made over the last year, core criteria and triennial criteria.

The benefit to federal agencies and all participating 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 are able to amortize the budget cost over the three years. Additionally, any changes and critical requirements are audited for compliance annually.

This document also provides instructions for Entity PKI Policy Management Authorities (PMAs) for submitting their annual audit compliance packages.

2 AUDIT REQUIREMENTS

Participating PKI PMAs are responsible for ensuring that all PKI components are audited in accordance with requirements identified in the appropriate CP and Certification Practice Statement (CPS) as well as the details provided in this guide, regardless of how or by whom the individual PKI components are managed and operated. Components other than Certification Authorities (CAs) may be audited fully or by using a representative sample. If the auditor uses statistical sampling, all PKI components, PKI component managers, and operators shall be considered in the sample. All such samples will vary on an annual basis with the exception of reviewing previous compliance audit findings, with emphasis on discrepancies and deficiencies.

The audit compliance package submitted by a participating PKI PMA may represent one of three distinct types of audits that may be performed, depending on the implementation maturity of the Entity PKI. Newly-established PKIs seeking cross-certification that do not have an operational history may submit a package representing a day zero audit as part of their cross-certification documentation, but must submit a package representing a full audit within their first year of membership. PKIs with a history of operations should submit a package representing a full audit as part of their cross-certification documentation. Once a participating PKI has submitted a package representing a full audit, the participating PKI may submit either a package representing a full compliance audit or triennial compliance audit in subsequent years. Section 3 provides instructions for how to submit the audit package, regardless of which type of audit is performed.

A participating Bridge PKI PMA is responsible for ensuring that their member PKIs are also fully audited in accordance with comparable requirements. The Audit package for a Bridge PKI must state that they have up-to-date Audit Letters for all their members on file, if the member audit letters are not included in the audit package. Therefore, a Day Zero Compliance Audit shall not be sufficient for a new Bridge PKI.

2.1 DAY ZERO 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.

A Day Zero Compliance Audit is restricted for use when an experienced PKI operator is establishing a new PKI to participate in the FPKI. This may be due to requiring a new CP or CPS that meets the requirements for entry into the FPKI and the participating PKI intends to establish one or more new CAs that will be dedicated to serving their FPKI customer base.

A Bridge PKI Compliance Audit must include evidence that the Bridge is following their stated procedures for managing their member PKIs. Therefore, a Day Zero Compliance Audit shall not be sufficient for a new participating Bridge PKI.

2.2 FULL COMPLIANCE AUDIT

For a full compliance 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. If performed, a participating PKI may use initial compliance audit findings as part of the full first compliance audit. A full compliance audit from the previous year is required as the baseline for subsequent triennial audits.

2.3 TRIENNIAL COMPLIANCE AUDIT

In 2010 the FPKI Audit Working Group 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 of triennial controls. Each subset shall be audited for compliance once over the period of three years. The combination of annual core controls and triennial controls over three years may be substituted for a full compliance audit every year. The core controls are detailed in APPENDIX A. The triennial control subsets are as follows:

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

As part of a triennial compliance audit, the compliance auditor shall review previous compliance audit findings for associated changes and corrective actions, and shall review all changes in policy, procedures, personnel, 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.

The compliance auditor's assessment of findings shall be based on the Auditor Letter of Compliance, see APPENDIX B, and shall address the elements described in the Compliance Audit Cookbook, see APPENDIX D.

3 AUDIT REPORTING PROCESS

On an annual basis, each Entity PKI PMA shall submit an audit compliance package that addresses the requirements identified in this guidance. As part of this package, the participating PKI PMA shall assert that the audit report represents a complete audit of all components of the Entity PKI, including any that may be separately managed and operated.

The organization submitting the Audit must include an architectural overview or statement detailing the components included in that Entity's PKI with the cross-certified or subordinate relationship to the FPKI. This statement must include a list of the CAs and how the organization meets the requirements for Registration and Issuance (i.e., is the RA functionality managed by the organization or externally), what repositories/certificate status servers support the PKI, and if appropriate, what card management systems are employed and whether they are internally or externally managed. This statement is required in order for the FPKIPA to determine if the Audit Letter(s) received are sufficient for the entire PKI affiliated with the FPKI. SSPs shall also include a list of supported agencies so a determination can be made if all required annual Personal Identity Verification (PIV) card testing has been conducted.

For federal agencies, an up-to-date National Institute of Standards and Technology (NIST) Special Publication 800-79 assessment may be used to document audit assessments of the Registration Authority (RA) and Card Management System (CMS) functions for PIV.

The participating PKI PMA shall attach evidence of compliance provided by an independent compliance auditor for all PKI components. An audit compliance package must consist of one of the following:

1. A single Auditor Letter of Compliance, signed by the auditor, covering all PKI components and functions under the overall responsibility of the participating PKI PMA, including those that are separately managed and operated. A template for the Auditor Letter of Compliance can be found in APPENDIX B.
2. Multiple Auditor Letters of Compliance, signed by their respective auditors, covering the Principal CA and all PKI components and functions under the overall responsibility of the participating PKI PMA, including those that are separately managed and operated. A template for the Auditor Letter of Compliance can be found in APPENDIX B.
3. Both of the following:
 - a. An Auditor Letter of Compliance, signed by the auditor, covering the Principal CA and any other components (Certificate Status Servers (CSSs), CMSs, RAs) covered in that audit. A template for the Auditor Letter of Compliance can be found in APPENDIX B.
 - b. Auditor Compliance Summary(ies) signed by the auditor(s) who performed the summary review, covering all PKI components and functions not covered by the Principal CA Audit Letter. Each auditor conducting a summary review must be sufficiently organizationally separated from the Entity(ies) that performed the audits and from the participating PKI to provide an unbiased independent evaluation. A template for the Auditor Compliance Summary can be found in APPENDIX C.

In addition to providing evidence, the participating PKI PMA shall state that the FPKIPA may review full audit reports upon request.

APPENDIX D provides guidance regarding the criteria the FPKIPA will use in determining if the annual audit report is complete and compliant. Participating PKI PMAs are encouraged to use this guidance in preparing their annual compliance packages.

APPENDIX A FPKI ANNUAL CORE REQUIREMENTS¹

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	<p>The Entity CAs and/or RAs shall record the information set forth below for issuance of each certificate:</p> <ul style="list-style-type: none"> • 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. <p><i>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.</i></p>
3	RFC: 4.9.1	<p>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.</p> <p>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.</p>
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

¹ These requirements will need to be updated after the Certificate Policy update process is complete

No.	RFC Section	Control Statement
		stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.
8	RFC: 5.1.2	<p>The physical security requirements pertaining to CAs that issue Basic Assurance certificates are:</p> <ul style="list-style-type: none"> • 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 <p>Comments: This requirement applies to Basic, but is different than the Medium requirement</p>
9	RFC: 5.1.2	<p>The physical security requirements pertaining to CAs that issue Basic Assurance certificates are:</p> <ul style="list-style-type: none"> • 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 <p>In addition to those requirements, the following requirements shall apply to CAs that issue Medium, Medium Hardware, or High assurance certificates:</p> <ul style="list-style-type: none"> • 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 <p><i>Practice Note: Multiparty physical access control to CA equipment can be achieved by one 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.</i></p>
10	RFC: 5.1.2	<p>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:</p> <ul style="list-style-type: none"> • 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	<p>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.</p>

No.	RFC Section	Control Statement
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.
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	<p>Two or more persons are required per task for the following tasks:</p> <ul style="list-style-type: none"> • CA key generation; • CA signing key activation; • CA private key backup. <p>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.</p> <p>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.</p>
18	RFC: 5.2.4	<p>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.</p> <p>Comments: This requirement applies to Basic, but is different than the Medium requirement</p>
19	RFC: 5.2.4	<p>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.</p>

No.	RFC Section	Control Statement
20	RFC: 5.2.4	<p>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.</p> <p>Comments: This requirement applies to High, but not to Medium HW</p>
21	RFC: 5.3.1	<p>All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity.</p>
22	RFC: 5.3.1	<p>For Federal Agency PKIs, regardless of the assurance level, all trusted roles are required to be held by U.S. citizens.</p>
23	RFC: 5.3.2	<p>Entity CA personnel shall, at a minimum, pass a background investigation covering the following areas:</p> <ul style="list-style-type: none"> • Employment; • Education; • Place of residence; • Law Enforcement; and • References. <p>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.</p>
24	RFC: 5.3.3	<p>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.</p>
25	RFC: 5.3.3	<p>Personnel performing duties with respect to the operation of the Entity CA shall receive comprehensive training, or demonstrate competence, in the following areas:</p> <ul style="list-style-type: none"> • CA/RA security principles and mechanisms; • All PKI software versions in use on the CA system. <p>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.</p>
26	RFC: 5.3.4	<p>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.</p> <p>Documentation shall be maintained identifying all personnel who received training and the level of training completed.</p>
27	RFC: 5.3.7	<p>Contractor personnel employed to perform functions pertaining to an Entity CA shall meet the personnel requirements set forth in the Entity CP.</p>

No.	RFC Section	Control Statement
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	<p>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):</p> <ul style="list-style-type: none"> • 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.
32	RFC: 5.4.2	<p>Audit logs shall be reviewed as required for cause.</p> <p><i>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.</i></p> <p>Comments: This requirement applies to Basic, but is different than the Medium requirement</p>
33	RFC: 5.4.2	<p>Audit logs shall be reviewed at least once every two months</p> <p><i>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.</i></p> <p>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.</p>
34	RFC: 5.4.2	<p>Audit logs shall be reviewed at least once per month</p> <p>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.</p> <p>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</p>

No.	RFC Section	Control Statement
		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: <ul style="list-style-type: none"> • 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.
40	RFC: 5.4.8	For Entity CAs, personnel shall perform routine assessments for evidence of malicious activity. <i>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.</i>
41	RFC: 5.5.1	At a minimum, the following data shall be recorded for archive [BASIC] <ul style="list-style-type: none"> • CA accreditation (if applicable) • Certificate Policy • Certification Practice Statement • Contractual obligations • Other agreements concerning operations of the CA • System and equipment configuration • Modifications and updates to system or configuration • Certificate requests • Revocation requests

No.	RFC Section	Control Statement
		<ul style="list-style-type: none"> • Subscriber identity Authentication data as per Section 3.2.3 • Documentation of receipt and acceptance of certificates • Subscriber Agreements • Documentation of receipt of tokens • All certificates issued or published • Record of CA Re-key • All CRLs issued and/or published • Other data or applications to verify archive contents • Compliance Auditor reports • Any changes to the Audit parameters, e.g., audit frequency, type of event audited • Any attempt to delete or modify the Audit logs • Whenever the CA generates a key (Not mandatory for single session or one-time use symmetric keys) • All access to certificate subject private keys retained within the CA for key recovery purposes • All changes to the trusted public keys, including additions and deletions • The export of private and secret keys (keys used for a single session or message are excluded) • The approval or rejection of a certificate status change request • Appointment of an individual to a Trusted Role • Destruction of cryptographic modules • All certificate compromise notifications • Remedial action taken as a result of violations of physical security • Violations of Certificate Policy • Violations of Certification Practice Statement <p>Comments: This requirement applies to Basic, but is different than the Medium requirement Dup in Medium</p>
42	RFC: 5.5.1	<p>At a minimum, the following data shall be recorded for archive [MEDIUM]:</p> <ul style="list-style-type: none"> • CA accreditation (if applicable) • Certificate Policy • Certification Practice Statement • Contractual obligations • Other agreements concerning operations of the CA • System and equipment configuration • Modifications and updates to system or configuration • Certificate requests

No.	RFC Section	Control Statement
		<ul style="list-style-type: none"> • Revocation requests • Subscriber identity Authentication data as per Section 3.2.3 • Documentation of receipt and acceptance of certificates • Subscriber Agreements • Documentation of receipt of tokens • All certificates issued or published • Record of CA Re-key • All CRLs issued and/or published • Other data or applications to verify archive contents • Compliance Auditor reports • Any changes to the Audit parameters, e.g., audit frequency, type of event audited • Any attempt to delete or modify the Audit logs • Whenever the CA generates a key (Not mandatory for single session or one-time use symmetric keys) • All access to certificate subject private keys retained within the CA for key recovery purposes • All changes to the trusted public keys, including additions and deletions • The export of private and secret keys (keys used for a single session or message are excluded) • The approval or rejection of a certificate status change request • Appointment of an individual to a Trusted Role • Destruction of cryptographic modules • All certificate compromise notifications • Remedial action taken as a result of violations of physical security • Violations of Certificate Policy <p>Violations of Certification Practice Statement</p>
43	RFC: 5.7.3	<p>If the Entity CA signature keys are compromised or lost (such that compromise is possible even though not certain):</p> <ul style="list-style-type: none"> • [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. <p>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.</p>
44	RFC: 5.7.3	<p>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.</p>

No.	RFC Section	Control Statement
45	RFC: 6.1.1	<p>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.</p> <p><i>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.</i></p>
46	RFC: 6.1.1	<p><i>[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.</i></p> <p>[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.</p> <p>Comments: Not Basic</p>
47	RFC: 6.1.2	<p>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:</p> <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> ○ For hardware modules, accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it. ○ 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. <p>The Entity CA must maintain a record of the subscriber acknowledgement of receipt of the token.</p>
48	RFC: 6.2.9	<p>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.</p>
49	RFC: 6.5.1	<p>The Entity CA and its ancillary parts shall include the following functionality:</p> <ul style="list-style-type: none"> • authenticate the identity of users before permitting access to the system or applications; • manage privileges of users to limit users to their assigned roles;

No.	RFC Section	Control Statement
		<ul style="list-style-type: none"> • 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. <p><i>These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards</i></p>
50	RFC: 6.5.1	<p>For Certificate Status Servers, the computer security functions listed below are required:</p> <ul style="list-style-type: none"> • 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	<p>The System Development Controls for the Entity CAs are as follows:</p> <ul style="list-style-type: none"> • Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment. Hardware and software shall be <u>scanned</u> for malicious code on first use and periodically thereafter.
52	RFC: 6.6.2	<p>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.</p>
53	RFC: 6.7	<p>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.</p>
54	RFC: 8.1	<p>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.</p>
55	RFC: 8.2	<p>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.</p>

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: <ul style="list-style-type: none"> • 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 requirement.

FBCA 5.4.1 – Types of Events Recorded [BASIC]

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

	Auditable Event	Basic	Medium (All Policies) and High
	TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE		
15	All changes to the trusted public keys, including additions and deletions	X	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 excluded)	X	X
	CERTIFICATE REGISTRATION		
18	All certificate requests	X	X
	CERTIFICATE REVOCATION		
19	All certificate revocation requests	X	X
	CERTIFICATE STATUS CHANGE APPROVAL		
20	The approval or rejection of a certificate status change request	X	X
	ENTITY CA CONFIGURATION		
21	Any security-relevant changes to the configuration of the Entity CA	X	X
	ACCOUNT ADMINISTRATION		
22	Roles and users are added or deleted	X	X
23	The access control privileges of a user account or a role are modified	X	X
	CERTIFICATE PROFILE MANAGEMENT		
24	All changes to the certificate profile	X	X
	REVOCATION PROFILE MANAGEMENT		
25	All changes to the revocation profile	X	X
	CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT		
26	All changes to the certificate revocation list profile	X	X
	MISCELLANEOUS		
27	<i>Appointment of an individual to a Trusted Role</i>	X	X
28	<i>Designation of personnel for multiparty control</i>		X
29	<i>Installation of the Operating System</i>	X	X
30	<i>Installation of the Entity CA</i>	X	X
31	<i>Installing hardware cryptographic modules</i>		X
32	<i>Removing hardware cryptographic modules</i>		X
33	<i>Destruction of cryptographic modules</i>	X	X
34	<i>System Startup</i>	X	X
35	<i>Logon Attempts to Entity CA Apps</i>	X	X
36	<i>Receipt of Hardware / Software</i>		X
37	<i>Attempts to set passwords</i>	X	X
38	<i>Attempts to modify passwords</i>	X	X
39	<i>Backing up Entity CA internal database</i>	X	X
40	<i>Restoring Agency CA internal database</i>	X	X
41	<i>File manipulation (e.g., creation, renaming, moving)</i>		X
42	<i>Posting of any material to a repository</i>		X
43	<i>Access to Entity CA internal database</i>		X
44	<i>All certificate compromise notification requests</i>	X	X
45	<i>Loading tokens with certificates</i>		X
46	<i>Shipment of Tokens</i>		X
47	<i>Zeroizing tokens</i>	X	X
48	<i>Rekey of the Entity CA</i>	X	X
	<i>Configuration changes to the CA server involving:</i>		

	Auditable Event	Basic	Medium (All Policies) and High
49	<i>Hardware</i>	X	X
50	<i>Software</i>	X	X
51	<i>Operating System</i>	X	X
52	<i>Patches</i>	X	X
53	<i>Security Profiles</i>		X
	PHYSICAL ACCESS / SITE SECURITY		
54	<i>Personnel Access to room housing Entity CA</i>		X
55	<i>Access to the Entity CA server</i>		X
56	<i>Known or suspected violations of physical security</i>	X	X
	ANOMALIES		
57	<i>Software Error conditions</i>	X	X
58	<i>Software check integrity failures</i>	X	X
59	<i>Receipt of improper messages</i>		X
60	<i>Misrouted messages</i>		X
61	<i>Network attacks (suspected or confirmed)</i>	X	X
62	<i>Equipment failure</i>	X	X
63	<i>Electrical power outages</i>		X
64	<i>Uninterruptible Power Supply (UPS) failure</i>		X
65	<i>Obvious and significant network service or access failures</i>		X
66	<i>Violations of Certificate Policy</i>	X	X
67	<i>Violations of Certification Practice Statement</i>	X	X
68	<i>Resetting Operating System clock</i>	X	X

APPENDIX B AUDITOR LETTER OF COMPLIANCE TEMPLATE

These requirements apply to all Federal PKI participating PKIs, including members of the Federal Bridge and CAs operating under the Common Policy.

The Auditor Letter of Compliance shall be addressed to the participating PKI PMA and shall be signed by the auditor.

NOTE: *The signature is typically the corporate signature of the audit firm or the signature of the head of the independent office within the participating PKI organization (e.g., the organization's Inspector General).*

The following background information about the auditor is required:

- Identity of the Auditor(s) and the individuals performing the audit;
- Competence of the Auditor(s) to perform compliance audits as required by the applicable CP and CPS;
- Experience of the individuals performing the audit in auditing PKI systems as required by the applicable CP and CPS;
- Relationship of the Auditor(s) to the participating PKI PMA and the entity operating the component(s) being audited. This relationship must clearly demonstrate the independence of the Auditor(s) as required by the applicable CP and CPS

The following information regarding the audit itself is required.

- The date the audit was performed.
- The period of performance the audit covers.
- Whether a particular methodology was used, and if so, what methodology.
- Which entity PKI component(s) were audited (CAs, CSSs, CMSs, and RAs).
- Which documents were reviewed as a part of the audit, including document dates and version numbers.

The following audit information is required summarizing the results of the audit:

- A statement that the operations of the audited component(s) were evaluated for conformance to the requirements of its CPS.
- Report the findings of the evaluation of operational conformance of the audited component(s) to the applicable CPSs.
- A statement that CPS was evaluated for conformance to the entity PKI's CP.
- Report the findings of the evaluation of the CPS conformance to the entity PKI CP.
- If applicable (always applicable for the participating PKI's Principal CA), a statement that the operations of the component(s) were evaluated for conformance to the requirements of all cross-certification Memorandum of Agreement (MOAs) executed by the participating PKI with other entities.
- If applicable (always applicable for the participating PKI's Principal CA), report the findings of the evaluation of the component(s) conformance to the requirements of all cross-certification MOAs executed by the participating PKI.

Special Requirements for Auditing New CAs (Day Zero Audit)

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

- State which procedures have been performed using the operational system and could be fully evaluated for conformance to the requirements of the PKI CPS.
- Report the findings of the evaluation.
- State which procedures have not been performed on the operational system and were evaluated for conformance to the requirements of the PKI CPS, but only with respect to training and written procedures.
- Report the findings of the evaluation.
- State that the PKI's CPS was evaluated for conformance to the supported certificate policies.
- Report the findings of the evaluation.

Notes on Audit Methodology

Since the Federal Bridge Certification Authority (FBCA) and Common Policy CPs are neutral as to audit methodology, any audit approach is acceptable provided that the requirements of the Certificate Policy and this document are addressed.

At the present time, a default WebTrust for CA audit will not satisfy the requirements set forth above. To meet FBCA and 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 participating PKI. 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 participating 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 designated representatives and working groups.*

APPENDIX C AUDITOR COMPLIANCE SUMMARY TEMPLATE

These requirements apply to all Federal PKI cross-certified entities, including members of the Federal Bridge and CAs operating under the Common Policy.

The Auditor Compliance Summary is used when a participating PKI chooses to submit a single summary report for components that are independently audited rather than submit a separate audit letter for each audit. The Auditor Compliance Summary is generated by an independent auditor who reviews the audit reports or audit letters on file and provides a summary statement that the FPKIPA or its designated representatives can use to determine audit compliance.

The Auditor Compliance Summary shall be addressed to the participating PKI PMA and shall be signed by the auditor.

The cover letter for the Auditor Compliance Summary shall include the following background information about the auditor who wrote the summary:

- Identity of the Auditor(s) performing the Auditor Compliance Summary;
- Competency of the Auditor(s) to perform compliance audits as required by the applicable CP and CPS;
- Experience of the Auditor(s) in auditing PKI systems as required by the applicable CP and CPS;
- Relationship of the Auditor(s) to the participating PKI PMA and the entity operating the component(s) being audited. The auditor conducting the audit review must be sufficiently organizationally separated from the entity that performed the audits and from the participating PKI to provide an unbiased independent evaluation.

The following information is required for each audit report or audit letter reviewed.

Requirement	Response
Component(s) Covered by Audit <i>List the components that were included in the scope of the audit, including CAs, CMSs, CSSs, and/or RAs.</i>	
Audit Date <i>State the date the audit was performed.</i>	
Audit Review Period <i>State the dates covered by the audit.</i>	
Audit Methodology <i>If a specific audit methodology was performed, state the methodology.</i>	
Auditor Identity <i>State the individual(s) names who performed the audit along with any relevant organization information.</i>	
Auditor Experience <i>State information provided by the auditor regarding relevant credentials, IT or IT Security experience, and experience with auditing PKI components.</i>	
Auditor Independence <i>State the relationship between the auditor, the PKI PMA,</i>	

<p><i>and the component(s) covered by the audit.</i></p>	
<p>Audit Documentation Scope <i>List the documents that were used in the audit to determine compliance, including document dates and version numbers. The CPS must be included. The CP should be included. If the CP is not included in the scope of the audit, provide a description for how CPS compliance to the CP was determined.</i></p>	
<p>Audit Documentation Findings <i>State whether the audit found that the CPS conformed to the CP. If the audit did not find that the CPS conformed, provide information regarding deficiencies found.</i></p>	
<p>Audit Operation Findings <i>State whether the audit found that the component(s) conformed to the requirements in the appropriate CPSs. If the audit did not find that the operations conformed, provide information regarding deficiencies found.</i></p>	
<p>Audit MOA Findings <i>If the component(s) are impacted by requirements in any cross-certification Memoranda of Agreement (MOA) executed by the Entity PKI, state whether the audit found that the component(s) conformed to the requirements in the MOAs. If the audit did not find that the operations conformed, provide information regarding deficiencies found.</i></p>	
<p>Audit Signature <i>State whether the audit report was signed by the auditor.</i></p>	

APPENDIX D THE ANNOTATED COMPLIANCE AUDIT COOKBOOK

This section shows guidance, questions, and comments that are used in determining whether annual audit compliance packages, including Auditor Letters of Compliance and Auditor Compliance Summaries are complete and compliant. Note that determination of compliance with the Federal PKI is the responsibility of the FPKIPA.

Requirement	Response
<p>Are all Component(s) Covered by Audit?</p> <p>1) <i>Does architectural overview match FPKIPA's understanding of the entity's PKI (eg. All CAs found by AIA Webcrawler for the cross-certified CA are included; RA, repository/CSS and CMS responsibility are included)</i></p> <p>2) <i>Are all identified components covered by Audit Letter(s) received</i></p>	<p>Was a cover letter (email) submitted that clearly states what components of the PKI are covered by the associated Audit Letter(s) and whether there are any additional components of the member's PKI that are not covered in this audit package?</p>

Audit Guidance	Commentary
<p>Components Covered by Audit For PKIs with multiple components, state whether evidence of audit reports for all components has been provided</p>	<p>Was audit evidence through Auditor Letters of Compliance and Auditor Compliance Summaries provided for your review for all PKI components?</p>
<p>Audit Date The date the audit was performed</p>	<p>Did each Auditor Letter of Compliance and Auditor Compliance Summary indicate the dates when the audits were 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.</p>
<p>Audit Review Period State the dates covered by the audit.</p>	<p>Did each Auditor Letter of Compliance and Auditor Compliance Summary indicate the dates covered by the audit? As a reality check, if the audit is performed in May of 2009, the date covered should include the previous 12 months. This period may be shorter than 12 months if the PKI is newly established or may be slightly longer if there was a delay in scheduling the audit. However, there should not be a significant gap between the previous audit letter for the same components and this one.</p>
<p>Audit Methodology Whether a particular methodology was used, and if so, what methodology.</p>	<p>Did each Auditor Letter of Compliance and Auditor Compliance Summary indicate if a particular audit methodology was used; and if so, what methodology? At the present time, the FPKI is methodology neutral.</p>
<p>Auditor Identity Identity of the Auditor and the individuals performing the audits</p>	<p>Did each Auditor Letter of Compliance and Auditor Compliance Summary identify the auditor and the individuals performing the audit? Many of the big auditing concerns are partnerships or corporations that assert that the <u>corporate entity</u> performed the audit. While that's true in one sense, the FPKIPA wants the individual auditors identified – see the following regarding competence and experience.</p>

Audit Guidance	Commentary
<p>Auditor Experience The auditor must be a Certified Information System Auditor (CISA) or IT security specialist, and a PKI subject matter specialist [see also FPKI and Common Policy CP Section 8.2]</p>	<p>Did each Auditor Letter of Compliance and Auditor Compliance Summary provide sufficient information for the FPKIPA to determine the competence and experience of the auditor? Individuals have competence, partnerships and corporations do not. The FPKIPA is looking for the individual auditor’s credentials here. 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.</p>
<p>Auditor Independence 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.</p>	<p>Did each Auditor Letter of Compliance and Auditor Compliance Summary provide sufficient information for the FPKIPA to determine the relationship and independence of the auditor to the PKI Entity that was audited? The Auditor needs to be independent and not conflicted. If there were multiple auditors auditing different components, each auditor must be independent both of the Entity PKI PMA and of the entity operating the components being audited.</p>
<p>Audit Documentation Scope Which documents were reviewed as a part of the audit, including document dates and version numbers.</p>	<p>Did each Auditor Letter of Compliance and Auditor Compliance Summary provide a full list of relevant documents (i.e., CP, CPS, MOA) that were reviewed for each audited component, including dates and version numbers? At a MINIMUM the CP and CPS should be identified here – as well as any other documents relied upon in conducting the audit.</p>
<p>Audit Documentation Findings State that the CPS for the Principal CA and any other CPSs used by the Entity PKI were evaluated for conformance to the Entity PKI’s CP. Report the findings of the evaluation of the CPSs conformance to the Entity PKI’s CP.</p>	<p>Did each Auditor Letter of Compliance and Auditor Compliance Summary state that the applicable CPS(s) were evaluated for conformance to the entity PKI’s CP? Did each Auditor Letter of Compliance and Auditor Compliance Summary state the findings of the evaluation of the applicable CPS for conformance to the entity PKI CP, including details of any discrepancies found? 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 FPKIPA would like to know about it. If a CPS is not 100% in accordance with the CP, the FPKIPA will want details on what’s deficient.</p>
<p>Audit Operation Findings State that the operations all Entity PKI components (Principal CA, other CAs, CSSs, CMSs, and RAs) were evaluated for conformance to the requirements of the applicable CPS. Report the findings of the evaluation of operational conformance to the applicable CPS.</p>	<p>Did each Auditor Letter of Compliance and Auditor Compliance Summary state whether the operations of the entity PKI components were evaluated for conformance to the requirements of the applicable CPS? Did each Auditor Letter of Compliance and Auditor Compliance Summary state the findings of the evaluation of operational conformance to the applicable CA CPS, including details of any discrepancies found?; 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. If the operations are not 100% in accordance with the CPS, the FPKIPA will want details on what’s deficient.</p>

Audit Guidance	Commentary
<p>Audit MOA Findings State that the operations of the Entity PKI's Principal CA and any other relevant components were evaluated for conformance to the requirements of all current cross-certification MOAs executed by the Entity PKI with other entities. Report the findings of the evaluation of the conformance to the requirements of all current cross-certification MOAs executed by the Entity PKI.</p>	<p>Did each applicable Auditor Letter of Compliance and Auditor Compliance Summary state that the relevant Entity PKI components were evaluated for conformance to the requirements of all current cross-certification MOAs executed by the Entity PKI with other entities? Did each applicable Auditor Letter of Compliance and Auditor Compliance Summary state the findings of the evaluation of conformance with applicable MOAs, including details of any discrepancies found? In many instances, the MOA imposes requirements on CAs or other PKI components. These should be examined. If there is anything other than 100% compliance with MOA imposed requirements, the FPKIPA would like to know about it.</p>
<p>Audit Signature Each auditor letter of compliance and audit review report is prepared and signed by the auditor.</p>	<p>Was each Auditor Letter of Compliance and Auditor Compliance Summary prepared and signed by the auditor? Did Auditor Compliance Summaries indicate that audit reports reviewed were also signed by their respective auditors? 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.</p>