CRYPTOCURRENCY
SECURITY STANDARD

CCSSA-PR Peer Review Guidance

Document History and Version History

Date	Document Version	Standard Version	Description
August 2024	v1.0	CCSS v8.1	Initial document developed by Marc Krisjanous CCSSA.

Introduction

The CCSS peer review process is unique in the domain of information security audits. With other audits, another auditor within the same organization auditing the entity does the peer review and, therefore, has access to the evidence. The fact that C4 requires an external entity to conduct the peer review is very unusual, and probably any client used to ISO27001, SOC 2 and PCI DSS audits will not have a process to deal with this and may assume that the peer reviewer is under the same NDA as the CCSSA, which they are not. To protect all parties involved, this guidance document outlines expectations for the peer review process.

Purpose of Guidance

This guidance ensures that the CCSSA, CCSSA-PR, and audited entity know their roles and the processes required for the peer review.

The guidance will address:

1. The difference between the CCSSA's first peer review and subsequent peer reviews.
2. What is to be peer-reviewed from the audit process.
3. The roles involved in the peer review process.
4. How to plan for a peer review.
5. How to establish a communication plan and set expected key milestones during the peer review process.

Purpose of Peer Review

The peer review process for a CCSS audit is unique compared to other audit methodologies and approaches to quality assurance for audit reports. To gain CCSS certification, the Report on Compliance (RoC), created by the CCSSA undertaking the audit, must have the redacted RoC peer-reviewed by another CCSSA with no prior or current relationship with the CCSSA or audited entity. This differs from other audit and certification processes as, generally, the quality assurance or peer review is undertaken by another auditor within the same organization.

To enforce this approach, C4 will generate a random list of CCSSAs from the list of registered CCSSAs, called the Peer Reviewer Options List (PROL), that the CCSSA undertaking the audit can contact and establish a peer review. The random list will not include other CCSSAs from the same organization as the CCSSA undertaking the audit.

The core benefits of the peer review process for a CCSS audit are:

- Consistency of CCSS audit and audit report
- An additional layer of quality assurance
- Reinforces the credibility of the CCSS certification
- Help protect C4 and CCSS brand

First Audit and the Peer Review Process

When a CCSSA conducts their first audit the peer review process will be conducted by a CCSS Steering Committee member. This ensures that the CCSSA upholds the high standard of auditing and reporting of CCSS audits that other CCSSAs, C4, the CCSS Steering Committee and other stakeholders expect.

For the CCSSA's first audit, after the CCSSA completes the Intent to Audit form, they will receive contact information for a CCSS Steering Committee Member from C4.

Peer Review Roles and Responsibilities

CCSSA

The responsibilities of the auditing CCSSA during the peer review process are:

1. Contact CCSSAs from the Peer Reviewer Options List (PROL) generated by C4 to determine an available and compatible CCSSA-PR to peer review the redacted RoC. If a CCSSA cannot find a suitable CCSSA from the PROL, then the CCSSA will contact C4, which will generate another PROL. NOTE! The CCSSA cannot select another CCSSA not on the PROL provided by C4.
    a. If this is the first audit of the CCSSA, then the list provided by C4 will only contain a CCSS Steering Committee member.

2. Seek a statement of work or other contractual arrangement to establish a formal work contract from the CCSSA selected from the PROL.

3. Ensure that the audited entity has reviewed and approved in writing the release of the redacted RoC that will be made available to the CCSSA-PR before the CCSSA-PR has

access to the redacted RoC.

4. Ensure the CCSSA-PR is only provided with the **redacted** RoC for peer review.
5. Ensure that the CCSSA-PR is not provided access to any audit evidence artifacts.
6. Ensure the Communication Plan has been created and approved by the CCSSA and the CCSSA-PR.
7. Ensure the Access Control Plan has been created and approved by the CCSSA and CCSSA-PR.

CCSSA-PR

The responsibilities of the CCSSA-PR during the peer review process:

1. Ensure that the redacted RoC shared by the CCSSA or audited entity is secure from unauthorized access.
2. Ensure that the Communication Plan agreed between the CCSSA and the CCSSA-PR is honored.
3. Do not contact the audited entity directly[1].
4. Do not discuss any part of the redacted RoC with anyone.
5. Ensure that the official C4 Report on Compliance (RoC) has been used by the CCSSA for the audit findings. The CCSSA MUST use the official C4 RoC template. The CCSSA-PR MUST NOT accept any audit report that has not used the official C4 RoC template.

[1] The task of the CCSSA-PR is to ascertain that the CCSSA conducted enough evidence-gathering techniques. If the CCSSA interviewed key personnel, reviewed documentation, observed processes and inspected configurations and systems, then there is a good chance that the CCSSA conducted enough evidence gathering techniques during the audit to form an opinion for a requirement. If the CCSSA missed any systems/components/services, for example, after all the evidence-gathering techniques were applied, this is the CCSSA's risk.

If a CCSSA-PR has concerns about an audited entity, CCSS audit, or CCSSA, use the Dispute Resolution process detailed in the Auditor Guide.

Audited Entity

The responsibilities of the audited entity during the peer review process are:

1. Do not communicate directly with anyone who states they are the CCSSA-PR or another CCSSA who is part of the audit. The only point of conduct is the CCSSA with whom the audited entity entered contractual arrangements to conduct a CCSS audit. If the entity has concerns regarding any part of the audit process, CCSSA, or CCSSA-PR, they may contact C4, keeping in mind that C4 has no involvement in the actual audit unless there is a dispute resolution needed to be resolved by the Steering Committee.

2. Do not share any audit evidence or proprietary information with anyone other than the contracted CCSSA.

Before the Peer Review

A kickoff meeting between the CCSSA and CCSSA-PR is highly recommended. The meeting can provide:

1. A general overview of the audited entity and the systems audited for CCSS compliance.

2. Establishing the Communication Plan and Access Control Plan.

3. If desired, an overview of the redacted RoC and other documentation such as a QSP SRoC and Responsibility Matrix.

Estimating Peer Review Effort (Hours)

Based on previous peer reviews, the estimated time to conduct a peer review is approximately 10 to 15 hours and varies depending on the system or systems being audited.

Communication Plan

After connecting with another CCSSA and forming a contractual arrangement with them to be the CCSSA-PR, a communication plan should be established between the CCSSA and CCSSA-PR. This plan should:

1. Establish the delivery date for both the draft and final peer review reports.

2. Determine when the CCSSA-PR will provide updates on the peer review process to the CCSSA.

3. Decide whether a draft version of the peer review report will be sent to the CCSSA, allowing for clarification, submission of additional requested evidence, or remediation before the final report is released by CCSSA-PR.

4. Outline how the CCSSA-PR can submit questions to the CCSSA.

5. Define the expected response time for the CCSSA to address questions submitted by the CCSSA-PR.

6. Specify how PR can address concerns related to the CCSSA's evidence-gathering techniques or other concerns regarding audit quality.

7. Detail the process for requesting additional hours to complete the peer review process.

8. Define the terms for handling time delays at the start and completion of the peer review process, whether caused by the CCSSA, CCSSA-PR, or the audited entity.

Access Control Plan

Even though the redacted RoC should have no confidential information remaining, there is still a risk that information that should not be made public may remain in the redacted RoC.

The redacted RoC must be treated as a confidential document by the CCSSA and CCSSA-PR. Before the CCSSA-PR has access to the redacted RoC, appropriate access controls must be implemented. The access controls that will be implemented must be agreed upon in writing by both the CCSSA and CCSSA-PR. This is called an Access Control Plan.

Access to the redacted RoC should be via access controls that require a password or another authentication factor. The password or other authentication token that grants access to the redacted RoC should be sent to the CCSSA-PR via another communication channel. For example, the redacted RoC could be zipped with a password and emailed to the CCSSA-PR. The password to the zip file is then sent via SMS.

Important note! The CCSSA and CCSSA-PR MUST NOT share any evidence collected from the audited entity.

Explanation of Redacted RoC

The redacted RoC is a copy of the completed RoC created by the CCSSA for the audit. C4 requires that another CCSSA with no professional or personal relationship with the CCSSA who conducted the audit undertake the peer review process of the CCSSA's audit reporting findings.

It is assumed that the CCSSA-PR will have no commercial or contractual relationship with the audited entity, including an NDA. Therefore, the CCSSA-PR is not legally allowed to view the full RoC or any of the evidence provided by the audited entity to the CCSSA.

Therefore, the CCSSA creates a copy of the RoC and redacts all sensitive information from the RoC such as:

1. All personally identifiable information (PII) of the assessed entities personnel involved in the audit such as first name, last name, email address, phone etc…

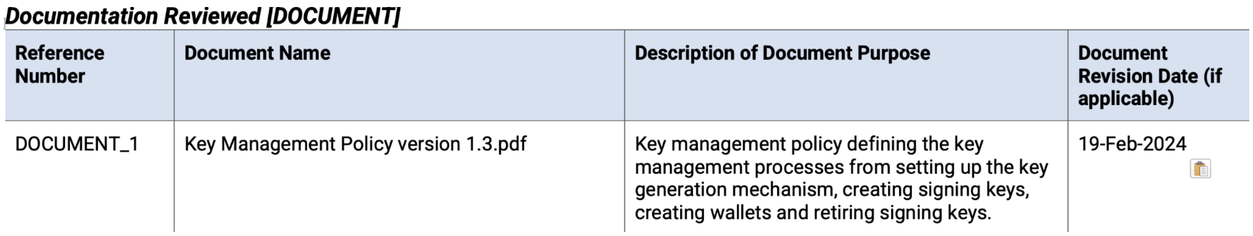
2. All sensitive information about the assessed entity must be redacted, including:
    a. Filenames of evidence artifacts that were collected and reviewed during the audit.
    b. Any diagrams, pictures, and screen captures showing sensitive information.
    c. Any other information within the audit report the CCSSA believes is sensitive and could impact the security of the assessed entity's environment if unauthorized users access the redacted RoC.

The audited entity should review the redacted RoC to ensure that all information the entity deems confidential is removed from the redacted RoC. The audited entity then must provide written permission to the CCSSA to release the redacted RoC to the CCSSA-PR.

Example of Redaction

The Audit Evidence section of the official C4 RoC template allows for the CCSSA to record evidence artifacts from the audit.

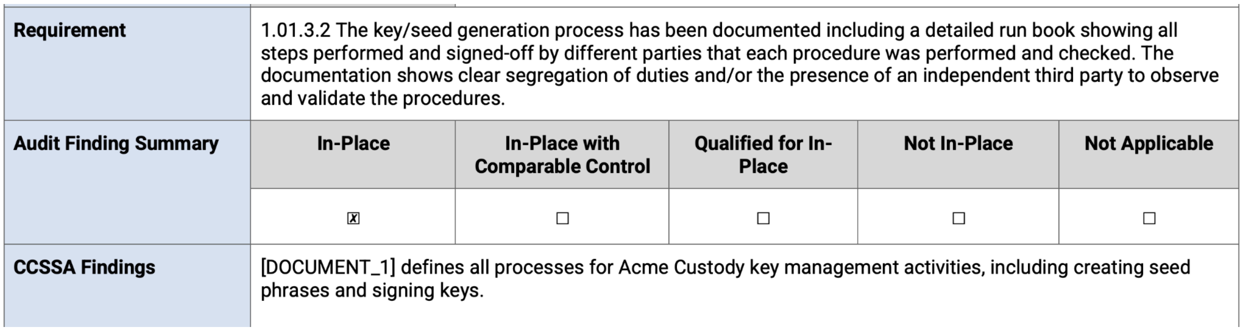
For example, a policy can be recorded in the "Document Reviewed" section and given a [DOCUMENT_] tag such as [DOCUMENT_1]. The [DOCUMENT_1] tag can then be used throughout the RoC as a reference when mentioning that particular policy.



Documentation Reviewed [DOCUMENT]

Reference Number	Document Name	Description of Document Purpose	Document Revision Date (if applicable)
DOCUMENT_1	Key Management Policy version 1.3.pdf	Key management policy defining the key management processes from setting up the key generation mechanism, creating signing keys, creating wallets and retiring signing keys.	19-Feb-2024

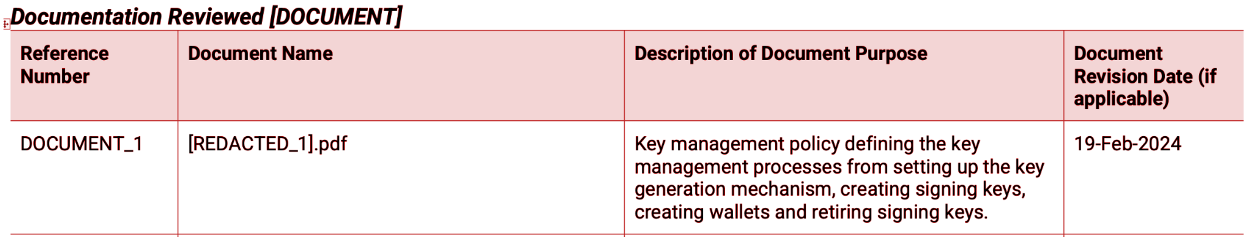
Figure 1 - The Key Management Policy document is recorded in the Document Review section



Requirement	1.01.3.2 The key/seed generation process has been documented including a detailed run book showing all steps performed and signed-off by different parties that each procedure was performed and checked. The documentation shows clear segregation of duties and/or the presence of an independent third party to observe and validate the procedures.				
Audit Finding Summary	**In-Place**	**In-Place with Comparable Control**	**Qualified for In-Place**	**Not In-Place**	**Not Applicable**
	☒	□	□	□	□
CCSSA Findings	[DOCUMENT_1] defines all processes for Acme Custody key management activities, including creating seed phrases and signing keys.				

Figure 2 - Using the [DOCUMENT_1] tag in the RoC requirements section.

When creating the redacted RoC, the CCSSA should redact the file name as this could be considered sensitive information that shows the entity's file naming convention.



Documentation Reviewed [DOCUMENT]

Reference Number	Document Name	Description of Document Purpose	Document Revision Date (if applicable)
DOCUMENT_1	[REDACTED_1].pdf	Key management policy defining the key management processes from setting up the key generation mechanism, creating signing keys, creating wallets and retiring signing keys.	19-Feb-2024

Figure 3 - The document file name is redacted only once.

Figure 3 shows that the document file name has been redacted only once because the [DOCUMENT_1] tag was used throughout the RoC instead of the file name. This saves time and effort for the CCSSA-PR in reviewing the redacted RoC.

NOTE: The CCSSA-PR must ensure that redactions do not obscure information critical to understanding the audit findings or the compliance status. The redactions must not hinder the report's transparency or accuracy.

Peer Review Process

CCSS Peer Review is an Open Peer Review type. It means that the identity of the CCSSA and the CCSSA-PR is known by all participants, during and after the review process. At the same time, comments and communication between CCSSA and CCSSA-PR are not publicly available. The transparency of Open Peer Review encourages accountability and civility, generally improving the overall quality of the review.

What Should be Received from the CCSSA?

Full System

If the audit is for a Full System that does not use a QSP then a reacted RoC is all that is required.

Full System with QSP

If the Full System has utilized a CCSS QSP as part of the information system, then the following will be expected:

- Redacted RoC
- QSP SRoC (the CCSSA needs this to work out what the QSP CCSS certification covers regarding CCSS requirements in place).

The QSP Responsibility Matrix should also be provided to the CCSSA-PR to help further identify the QSP's responsibilities and the QSP-certified system's user.

QSP

If the audit is for a QSP then a redacted RoC is all that is required.

Self-Custody

If the audit is for Self-Custody, then a redacted RoC is all that is required.

The Redacted RoC Sections

The CCSSA must use the official C4 Report on Compliance (RoC) template for the audit report, which can be downloaded via the CCSSA resources portal. The redacted RoC must also use the official C4 Report on Compliance (RoC) template.

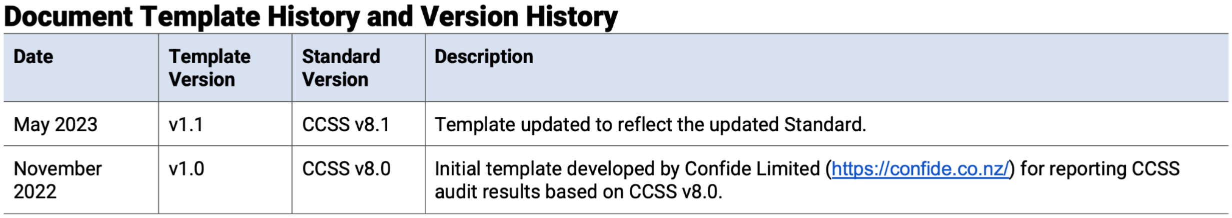
All sections of the Redacted RoC should be completed before submitting the redacted RoC to the CCSSA-PR for peer review.

The RoC, which is an official C4 audit document, must:

1. Have all CCSS requirements responded to. If a CCSS requirement does not apply to the audited entity, then “Not Applicable” must be entered for all subsections within the CCSS requirement section.

2. Remain unaltered, such as by changing the order of the sections, wording, formatting, and overall structure of the RoC template.

3. Be the latest version of the C4 official RoC. The CCSSA-PR must check that the CCSSA has used the latest version of the RoC by checking the current version available in the CCSSA Resources Portal and comparing that version of the RoC template with the version the CCSSA used.



Document Template History and Version History

Date	Template Version	Standard Version	Description
May 2023	v1.1	CCSS v8.1	Template updated to reflect the updated Standard.
November 2022	v1.0	CCSS v8.0	Initial template developed by Confide Limited (https://confide.co.nz/) for reporting CCSS audit results based on CCSS v8.0.

Figure 4 - The document template history section, which provides the version number of the RoC template.

The following sections are to be reviewed by the CCSSA-PR.

RoC Section	What is Expected
Contact Information	● The *Audited entity* table must be complete. ● The *CCSS Auditor (CCSSA)* table must be complete.
Summary of Audit	● The *Audit Testing Period* must have the dates of the start and finish of the audit. ● The *Demonstrated CCSS Level* must be complete, and the CCSS Level that was achieved and the CCSS designation (Full System, QSP or Self-Custody) must be provided. ● The *CCSSA Explanation of Level Audit* must be complete and document the roles, processes, and

	technology components that were interviewed, inspected, and reviewed to reach an opinion on the CCSS Level obtained. ● The *Aspect* table must be completed, checking the checkbox of the CCSS Level obtained for each CCSS aspect.
CCSS Trusted Environment Summary	● The *Trusted Environment* table must be completed, defining the people (roles), processes and technology components of the system(s) audited. ● A description of each component (the roles, processes and technology) that comprises the system(s) audited must be provided in reasonable detail so that a person who has no previous knowledge of the audited system(s) can understand the purpose and function of each component.
Validation of Trusted Environment	● The *Describe How the Trusted Environment was Validated* section must be completed to a reasonable level of detail so that a person who has no previous knowledge of the audited system(s) can understand how the CCSSA identified and confirmed the CCSS Trusted Environment and the essential components within the CCSS Trusted Environment. ● The *Provide the Name of the CCSSA who confirms that the validated environment has been accurately identified and included in the audit scope* section must be completed.
Evidence Retention	● The *Evidence Retention* table must be completed. ○ Any not applicable sections must be marked as “Not Applicable.” For example, if the CCSSA retains the evidence, these sections must be marked “Not Applicable”: ■ *Provide the name of the organization responsible for evidence retention* ■ *Provide the name of the assessor who confirms that the organization has been informed of the retention requirements* ■ *Provide the name of the member of the organization to attest that the evidence retention requirements will be met* ○ If the organization retains the evidence, the following sections must be completed. ■ *Provide the name of the assessor who confirms that the organization has been*

	informed of the retention requirements ■ *Provide the name of the member of the organization to attest that the evidence retention requirements will be met*
Detailed Findings	● All requirement tables must be completed in the *Detailed Findings* section. If a requirement is not applicable, then the "Not Applicable" findings status must be checked in the requirements *Audit Finding Summary* section. ● All requirements must have the *Audit Finding Summary* section completed. ● The *CCSSA Findings* section must describe how the CCSSA formed the findings status opinion (In-Place, In-Place with Comparable Control, Qualified for In-Place, Not In-Place, or Not Applicable) to a level of description that the CCSSA-PR can understand how the findings status opinion was reached. If the CCSSA-PR cannot understand how the findings status was reached based on the description provided, then the CCSSA must provide more information (of course, considering the confidentiality of the audited entity's environment). ● The *Evidence Gathered* section for each CCSS requirement must be completed for all requirements. If the evidence gathering technique was not implemented for a requirement, then "Not Applicable" must be written in the evidence gathering techniques section. ● If the evidence gathering technique was implemented for a requirement, the associated documentation of evidence or Reference Number is provided. Note that the *Audit Evidence* tables at the end of the RoC are used to record evidence collected and the "Reference Number" for that piece of evidence can be used in the "Evidence Gathered" section.
Audit Evidence - Interviews Conducted [INTERVIEW]	● Each person the CCSSA interviewed during the audit must be recorded in this section. ● The interviewee's name (first name, last name) must be redacted for privacy reasons as part of the redacted process. ● For each interview, the topics covered during the interview must be provided. ● The interviewee's role and the interviewee's entity must be completed. ● The Reference Number must be completed and be unique to the other evidence Reference Numbers for example, INTERVIEW_1, INTERVIEW_2,

	INTERVIEW_3.
Audit Evidence - Documentation Reviewed [DOCUMENT]	● Each document or file contains documentation such as policy, standard, procedure, BAU outputs (such as reports, log files, trace files, network captures), help guide, etc… must be recorded in this section. ● The document name must be provided, but if the file name contains sensitive information, then part or all of the file name must be redacted. For example, “HSM_092.Domain.com Pentest Report 20/July/2024” must be redacted so that the hostname is removed from the redacted RoC, for example “REDACTED Pentest Report 20/July/2024”. ● The *Description of Document Purpose* must be completed by providing a reasonable description so that the CCSSA-PR can ascertain the document's purpose. For example, “Pentest report for the HSM containing findings and updated remediation section”, “The entity's key management policy covering key generation, key rotation, key destruction”. ● If the document has versioning control, the last date reviewed must be provided. If the document does not have versioning control, then “Not Applicable” must be written. For example, a document containing the output of an HSM configuration dump created for the purposes of the audit will not have version control as it was generated expressly for the purposes of the CCSS audit. ● Each document recorded must have a unique “Reference Number” for example, DOCUMENT_1, DOCUMENT_2, DOCUMENT_3.
Audit Evidence - Process Observations [OBSERVATION]	● For each observation, the *Process Observed*, *Description of What Was Observed*, and *Date Observed* sections must be completed. ● The *Description of What Was Observed* section should provide enough detail so that the CCSSA-PR can understand the process that the CCSSA observed. ● Each observation recorded must have a unique “Reference Number” for example, OBSERVATION_1, OBSERVATION_2, OBSERVATION_3.
Audit Evidence - Inspections [INSPECTION]	● For each inspection, the *What Was Inspected*, *Inspection Findings*, and *Date Inspected* sections must be completed. ● The *What Was Inspected* must contain enough detail that the CCSSA-PR can understand what system(s) or

	configurations, etc... were inspected. ● Each inspection recorded must have a unique "Reference Number" for example, INSPECTION_1, INSPECTION_2, INSPECTION_3.
Audit Evidence - CCSS Committee Decisions [CCSS_DECISION]	● For each CCSS Steering Committee decision provided for the CCSSA, the *Evidence Presented*, *Date of CCSS Committee Decision*, *CCSSA Comments*, and *CCSS Committee Comments* sections must be completed. ● Each recorded CCSS Steering Committee decision must have a unique "Reference Number" for example, CCSS_DECISION_1, CCSS_DECISION_2, CCSS_DECISION_3.

Sample-Sets

Depending on the complexity of the in-scope environment, the CCSSA may either audit all people, process, and technology components or adopt a sampling methodology. The CCSS Audit Guide has a section (1.2.4) defining the sampling methodology.

If the CCSSA has applied a sampling approach to the audit, then the CCSSA-PR must review the sampling methodology used by the CCSSA for the audit and ensure it meets the sampling requirements in the CCSS Auditor Guide.

What is to be Peer Reviewed?

The CCSSA-PR will not have access to the unredacted RoC or evidence artifacts from the audit.

As mentioned in the "Peer Review Roles and Responsibilities - CCSSA-PR" section of this guidance, the CCSSA-PR is not reviewing the evidence artifacts or the full RoC. The CCSSA-PR is peer reviewing the redacted RoC to ascertain if the CCSSA conducted enough evidence gathering techniques for each CCSS requirement to form an opinion as to the findings status of a requirement (In-Place, In-Place with Comparable Control, Qualified for In-Place, Not In-Place or Not Applicable).

Four common evidence-gathering techniques are used for auditing information systems and information security management systems (ISMS).

1. Review - reviewing documentation such as policy, standards, and procedures is the most common evidence-gathering technique and is generally the first task of the CCSSA to help ascertain the people, processes, and technology components of an information

system and ISMS that are in scope for the CCSS audit. Documents to be reviewed may include:

a. A Policy is a formalized statement or document that outlines an entity's approach and commitments to securing its assets, data, and operations. It sets the overarching principles and rules that determine the desired security posture of the entity. An example of this is "*we will provide a secure environment for our customers to transact.*"
b. A Standard is a document that outlines best practices, based on internationally recognized standards, as to how the entity will meet a goal, such as "*the entity will implement strong access control mechanisms that conform to ISO27001 or NIST 800-53*" and another example "*the entity will use an HSM certified to FIPS 140-3*".
c. A Procedure details the specific actions or sequences of actions to be taken to implement a given security policy. They act as operational blueprints, providing clear instructions to staff or systems on how to perform tasks securely and consistently. For example, a procedure document can be used to onboard a new customer or configure a new HSM.

NOTE: concern should be raised by both the CCSSA and CCSSA-PR if an audited entity points to external documentation as their policy or standard. For example, an audited entity points to an open-source configuration guide on the project website for a mechanism or library as their standard. This should not be acceptable as the audited entity should ensure that internal documentation exists and not rely on external documentation outside of their control.

2. Interview - interviewing personnel responsible for and managing the in-scope systems is a vital evidence-gathering technique for a CCSSA. Interviewing personnel can highlight key information that is never located within written documentation, such as how work is really done - sometimes known as "Shadow IT". The key focus of interviewing personnel is understanding if the person interviewed is following the entity's policy/standards/procedures or doing something else. The "something" else will concern the CCSSA and the entity, as there will not be any oversight or control of what is actually being done and could introduce vulnerabilities into the in-scope environment.

3. Inspection - Inspection is an evidence-gathering technique where the CCSSA inspects system configurations and other technology components to ensure that configuration requirements stated in the standards and procedure documents have been implemented. For example, the entity states in its access control standard that all access into the in-scope environment must use MFA. The CCSSA should inspect the access control systems to ensure MFA has been implemented, configured correctly, and applied to all user accounts with access to the in-scope environment. Inspection is a "trust but

verify" approach to auditing where the documentation and interviewees state something is done, but the auditor needs to verify by inspecting the system.

4. Observation - observing a process being undertaken is another important evidence-gathering technique along the same lines as inspection - trust but verify. The CCSSA, if possible, should observe the processes being undertaken to ensure they meet the documented processes. For example, the CCSSA can observe personnel reviewing audit log files from in-scope systems or the process of adding a new user account to a system. When observing a process is impractical, such as asking the audited entity to undertake a key creation ceremony in production, the auditor should instead ask the personnel to discuss the steps that would be taken,

The CCSSA should use multiple evidence-gathering techniques to form an opinion on the status of a CCSS requirement. For example, consider this requirement below.

> *1.04.3.1 All key/seed holders have had their references checked prior to being trusted to hold one of the entity's keys/seeds.*

To ensure this requirement is "In-Place", the CCSSA could:

1. Review policies and/or standards that require all personnel with access to a signing key to have a reference check undertaken before access is granted.

2. Interview relevant personnel who are responsible for ensuring a reference check is undertaken.

3. Observe the process of conducting a reference check.

4. Review a sample of reference check reports.

For another example, consider the requirement below.

> *1.01.4.1 The cryptographic keys and seeds are created on a system with sufficient entropy to ensure the keys are not created with any bias towards a reduced range of values, or other deterministic properties.*

1. Review policies and/or standards that state a system that creates seeds and keys must have sufficient entropy. The policy and/or standard should also define what is "sufficient entropy".

    a. NOTE: The CCSSA must ensure that the mechanism that generates entropy meets the intent of this requirement, and this research should be documented in the redacted RoC so the CCSSA-PR can confirm that the CCSSA validated this.

2. Interview relevant personnel to confirm that the entropy mechanism is correctly configured and used for all seed and key generation.

3. Inspect the mechanism that generates the entropy, including any configuration options available and compare the current configurations to the vendor's documentation to ensure the configurations have been implemented based on the vendor's recommendations.

The two examples above demonstrate how applying more than one evidence gathering technique to a requirement should strengthen and provide a clear picture of whether the requirement is “In-Place” or not.

What is Not to be Peer Reviewed?

The following should not be part of the peer review process, unless there is agreement between the CCSSA and CCSSA-PR.

Grammar, Spelling, and Sentence Structure

CCSS certification is an international certification where a CCSSA and/or the audited entity may not have English as their first language. The CCSSA-PR should not spend time correcting the grammar, spelling, or sentence structure of the redacted RoC. As part of the peer review process the CCSSA must allow the audited entity to review the redacted RoC so the audited entity can check if all confidential and private information has been removed. If the audited entity has not raised concerns regarding the grammar, spelling etc.. to the CCSSA, then the CCSSA-PR must accept the redacted RoC as-is. However, there is a caveat: if the CCSSA-PR cannot understand or read what is being documented, the CCSSA-PR can report this to the CCSSA for remediation.

Text Formatting

The CCSSA-PR should not apply their formatting style to a redacted RoC. The role of the CCSSA-PR is not to format the redacted RoC according to their style preference but to make a formal opinion as the effort of the CCSSA in collecting evidence.

Changes (Fixes)

If during the CCSS peer review, the CCSSA-PR finds that some evidence-gathering techniques and/or the conclusions drawn from them were not adequate or more clarification is needed, then two possible approaches are:

1. The CCSSA-PR alerts the CCSSA to any questions about the evidence and/or conclusions provided as they arise during the peer review process. The CCSSA can then provide commentary and/or remediation during the peer review process. The goal of this option is to reduce multiple revisions of the peer review report. The only version of the peer review report is the final copy, as remediation was addressed during the peer review process. The redacted RoC may be shared and accessible by both the CCSSA and CCSSA-PR, allowing for inline commentary and updates in real-time.

2. Another option is to hold all questions and findings until the end of the initial peer review and release the peer review report to the CCSSA. The CCSSA then reviews the peer review report and makes changes to the RoC based on feedback, provides additional evidence, etc… then makes another copy of the updated RoC and submits the redacted RoC again for peer review. This option would be considered a more formal approach to peer review and would probably result in more time required for the peer review process to complete.

The Communication Plan created and agreed upon in the initial phase of the Peer Review should address these options and a preferred method agreed upon.

If the CCSSA and CCSSA-PR cannot come to an agreement on an audit finding, then C4 does provide a dispute process where the CCSS Steering Committee would review the position of the CCSSA and CCSSA-PR and provide a recommendation.

For more information on the C4 disputes process, please review section *1.3.5 Dispute Resolution* within the CCSS Auditor Guide

C4 Peer Review Report Template

As part of the Peer Review process, the CCSSA-PR must complete a *Peer Review Report* for the CCSSA using C4's CCSS *Peer Review Report Template*.

To ensure consistency, the peer review report template applies the same style and formatting elements as the official C4 *CCSS Audit template*.

You can download the official C4 Peer Review Report Template on C4's CCSSA Resource Page.

The Peer Review Report provides the following sections.

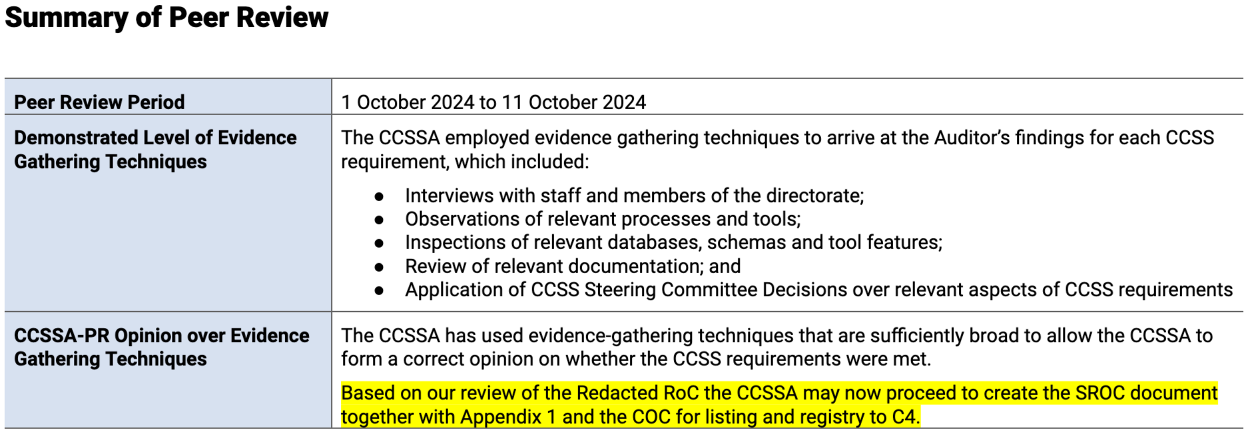
Peer Review Report Section	What is Expected
Contact Information	● The contact details of the CCSSA, CCSSA-PR and audited entity
Summary of Peer Review	● Complete the Peer Review Period - the time spent on the Peer Review. ● CCSSA-PR Approval to Proceed to the Next Stage in the Audit - this is where the CCSSA-PR provides the approval for the CCSSA to move to the next stage of the CCSS audit process. If approval is not given, explain why in this section.
Summary of Peer Review Findings	● The CCSSA-PR provides overall commentary on the redacted RoC, as well as recommendations, suggestions, etc.
CCSS Trusted Environment Summary	● Overview of CCSS Trusted Environment - The CCSSA-PR comments on whether the CCSSA has defined the CCSS Trusted Environment to a level required by CCSS. ● Validation of Trusted Environment - The CCSSA-PR comments on the effectiveness of the CCSSA to validate the CCSS Trusted Environment. ● Component section - the CCSSA-PR comments on the list of system components the CCSSA defined in the redacted RoC and if the other statements within the redacted RoC support the definitions.
Evidence Retention	● The CCSSA-PR confirms that the Evidence Retention section in the redacted RoC was completed.
Peer Review of Evidence Gathering Techniques	● For each CCSS requirement, a section is provided for the CCSSA-PR to complete. See "Peer Review of Evidence Gathering Techniques" section below for more detail.

Example Report Sections

This section provides examples of completed peer review report sections.

Summary of Peer Review Section

This section provides an example of a completed Summary of Peer Review.



Summary of Peer Review

Peer Review Period	1 October 2024 to 11 October 2024
Demonstrated Level of Evidence Gathering Techniques	The CCSSA employed evidence gathering techniques to arrive at the Auditor's findings for each CCSS requirement, which included: ● Interviews with staff and members of the directorate; ● Observations of relevant processes and tools; ● Inspections of relevant databases, schemas and tool features; ● Review of relevant documentation; and ● Application of CCSS Steering Committee Decisions over relevant aspects of CCSS requirements
CCSSA-PR Opinion over Evidence Gathering Techniques	The CCSSA has used evidence-gathering techniques that are sufficiently broad to allow the CCSSA to form a correct opinion on whether the CCSS requirements were met. Based on our review of the Redacted RoC the CCSSA may now proceed to create the SROC document together with Appendix 1 and the COC for listing and registry to C4.

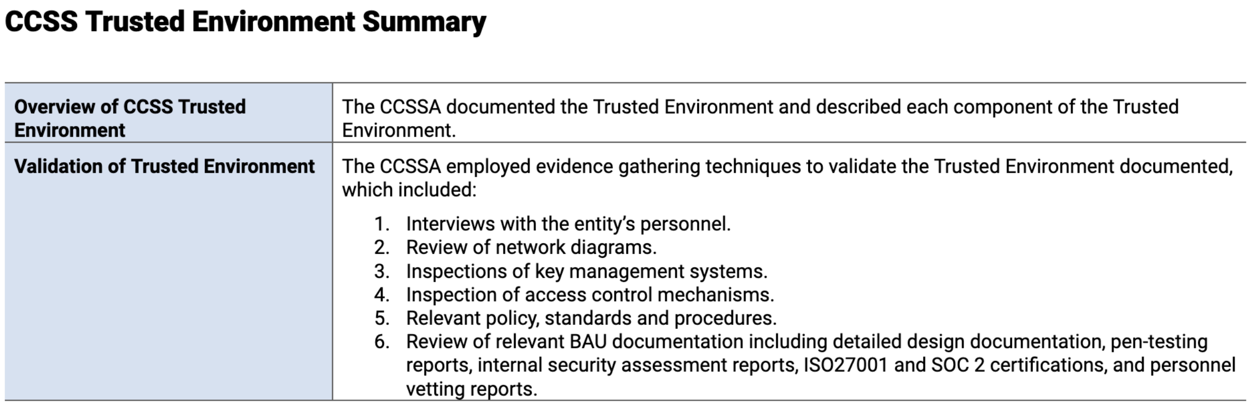
Figure 5 - Summary of Peer Review Section in Peer Review Report

Figure 5 shows a completed Summary of Peer Review section. The CCSSA-PR has provided their overall summary of the peer review process and whether the CCSSA conducted enough evidence gathering to reach the opinions made within the Redacted ROC.

Note that the highlighted text shows that the CCSSA-PR has officially stated that the peer review process is completed and that the CCSSA can proceed to the next step. This written confirmation to proceed is mandatory.

CCSS Trusted Environment Summary Section

This section provides an example of the completed CCSS Trusted Environment Summary section. Figure 6 shows that the CCSSA-PR has carefully reviewed the "CCSS Trusted Environment Summary - Trusted Environment" and "CCSS Trusted Environment Summary - Validation of Trusted Environment" sections within the Redacted ROC to ensure that the CCSSA validated the CCSS Trusted Environment scope for audit.



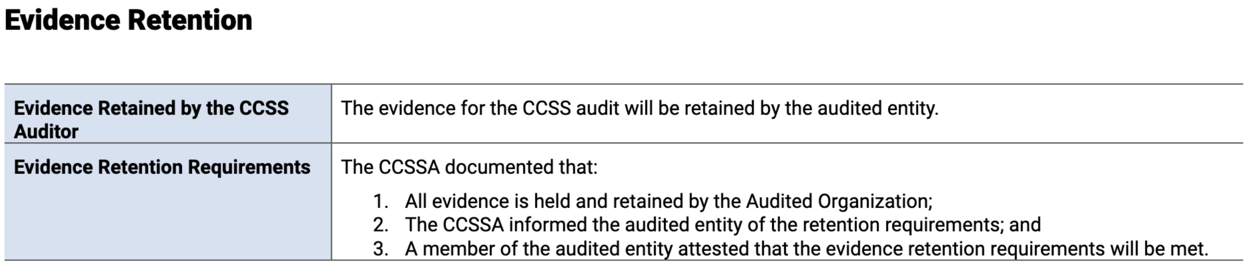
CCSS Trusted Environment Summary

Overview of CCSS Trusted Environment	The CCSSA documented the Trusted Environment and described each component of the Trusted Environment.
Validation of Trusted Environment	The CCSSA employed evidence gathering techniques to validate the Trusted Environment documented, which included: 1. Interviews with the entity's personnel. 2. Review of network diagrams. 3. Inspections of key management systems. 4. Inspection of access control mechanisms. 5. Relevant policy, standards and procedures. 6. Review of relevant BAU documentation including detailed design documentation, pen-testing reports, internal security assessment reports, ISO27001 and SOC 2 certifications, and personnel vetting reports.

Figure 6 - CCSS Trusted Environment Section in Peer Review Report

Evidence Retention Section

This section provides an example of the completed Evidence Retention section. Figure 7 shows that the audited entity, not the CCSSA, will retain the audit evidence.



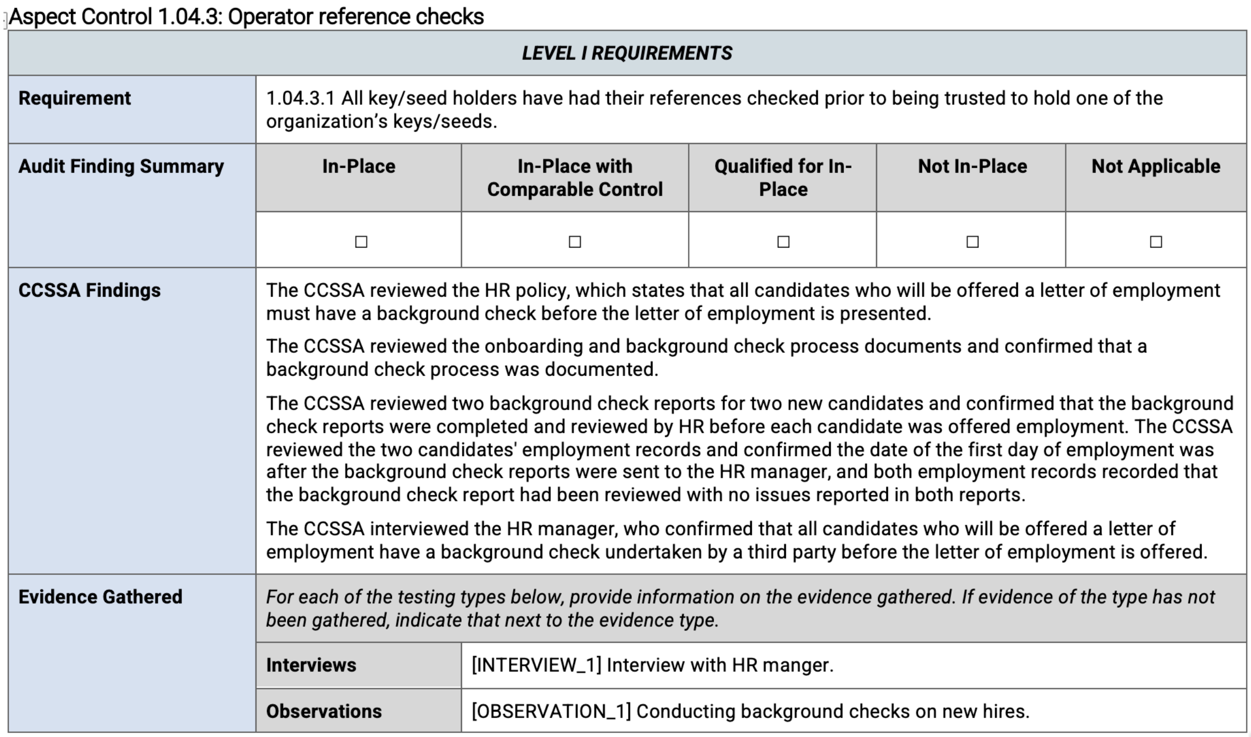
Evidence Retention

Evidence Retained by the CCSS Auditor	The evidence for the CCSS audit will be retained by the audited entity.
Evidence Retention Requirements	The CCSSA documented that: 1. All evidence is held and retained by the Audited Organization; 2. The CCSSA informed the audited entity of the retention requirements; and 3. A member of the audited entity attested that the evidence retention requirements will be met.

Figure 7 - Evidence Retention Section in Peer Review Report

Requirement Peer Review Findings Section

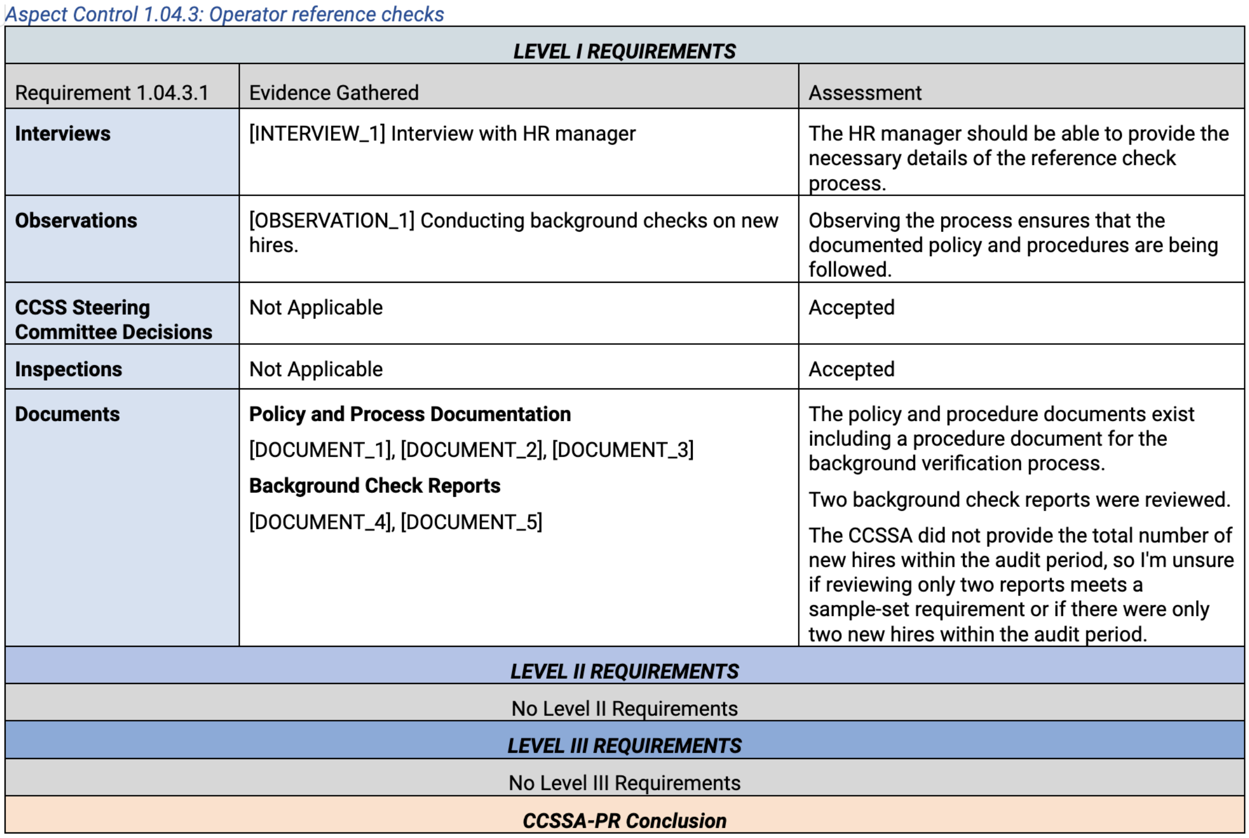
This section provides an example of a completed requirement peer review section. Figure 8 shows the requirement findings section for requirement 1.04.3.1 from the Redacted ROC, which is what the CCSSA-PR reviewed. Figures 9 and 10 display the peer review findings for requirement 1.04.3.1 within the peer review report completed by the CCSSA-PR.



Aspect Control 1.04.3: Operator reference checks

LEVEL I REQUIREMENTS					
Requirement	1.04.3.1 All key/seed holders have had their references checked prior to being trusted to hold one of the organization’s keys/seeds.				
Audit Finding Summary	**In-Place**	**In-Place with Comparable Control**	**Qualified for In-Place**	**Not In-Place**	**Not Applicable**
	□	□	□	□	□
CCSSA Findings	The CCSSA reviewed the HR policy, which states that all candidates who will be offered a letter of employment must have a background check before the letter of employment is presented. The CCSSA reviewed the onboarding and background check process documents and confirmed that a background check process was documented. The CCSSA reviewed two background check reports for two new candidates and confirmed that the background check reports were completed and reviewed by HR before each candidate was offered employment. The CCSSA reviewed the two candidates' employment records and confirmed the date of the first day of employment was after the background check reports were sent to the HR manager, and both employment records recorded that the background check report had been reviewed with no issues reported in both reports. The CCSSA interviewed the HR manager, who confirmed that all candidates who will be offered a letter of employment have a background check undertaken by a third party before the letter of employment is offered.				
Evidence Gathered	*For each of the testing types below, provide information on the evidence gathered. If evidence of the type has not been gathered, indicate that next to the evidence type.*				
	Interviews	[INTERVIEW_1] Interview with HR manger.			
	Observations	[OBSERVATION_1] Conducting background checks on new hires.			

Figure 8 - Extract of Requirement 1.04.3.1 Findings Section in the Redacted ROC



Aspect Control 1.04.3: Operator reference checks

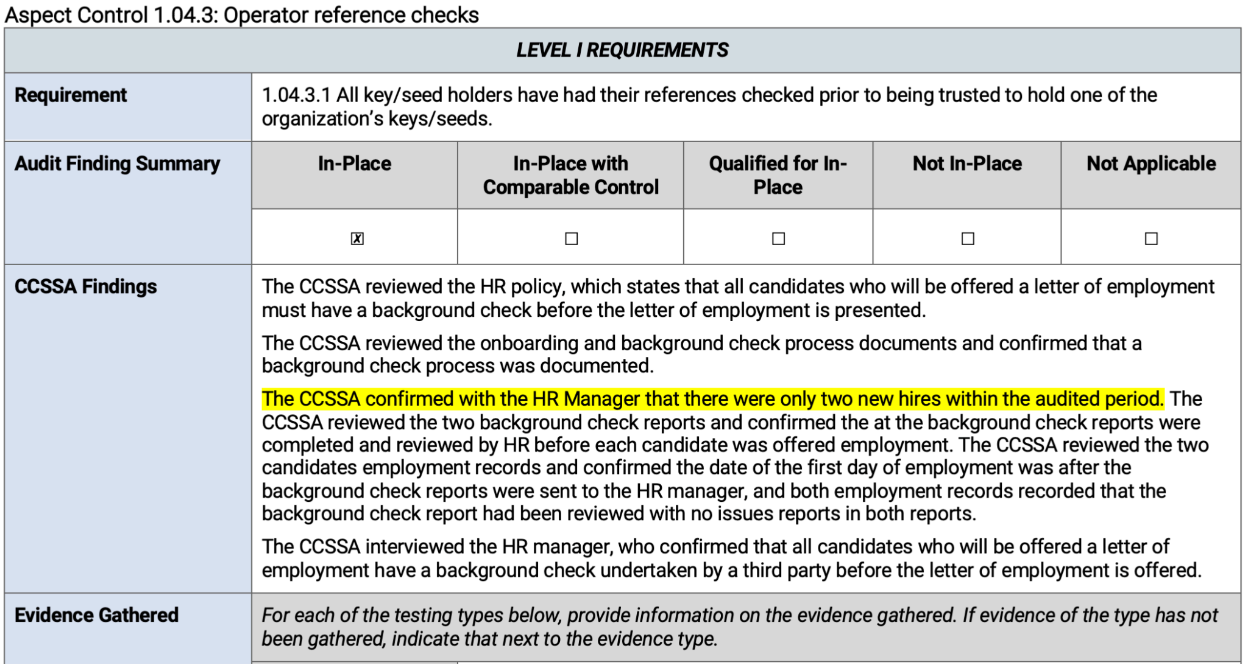
LEVEL I REQUIREMENTS		
Requirement 1.04.3.1	Evidence Gathered	Assessment
Interviews	[INTERVIEW_1] Interview with HR manager	The HR manager should be able to provide the necessary details of the reference check process.
Observations	[OBSERVATION_1] Conducting background checks on new hires.	Observing the process ensures that the documented policy and procedures are being followed.
CCSS Steering Committee Decisions	Not Applicable	Accepted
Inspections	Not Applicable	Accepted
Documents	**Policy and Process Documentation** [DOCUMENT_1], [DOCUMENT_2], [DOCUMENT_3] **Background Check Reports** [DOCUMENT_4], [DOCUMENT_5]	The policy and procedure documents exist including a procedure document for the background verification process. Two background check reports were reviewed. The CCSSA did not provide the total number of new hires within the audit period, so I'm unsure if reviewing only two reports meets a sample-set requirement or if there were only two new hires within the audit period.
LEVEL II REQUIREMENTS		
No Level II Requirements		
LEVEL III REQUIREMENTS		
No Level III Requirements		
CCSSA-PR Conclusion		

Figure 9 - Requirement 1.04.3.1 section in the Peer Review Report.

Figure 9 above provides an example of the CCSSA-PR queried in the Documents section whether the CCSSA collected all reference check reports conducted within the audit period or if this is only a sample of reports.

If the CCSSA and CCSSA-PR had defined in the Communication Plan that the CCSSA-PR can contact the CCSSA immediately with questions then the CCSSA-PR should ask the CCSSA to provide more detail for this requirement.

Depending on how the Redacted ROC is shared the CCSSA could update the copy directly.

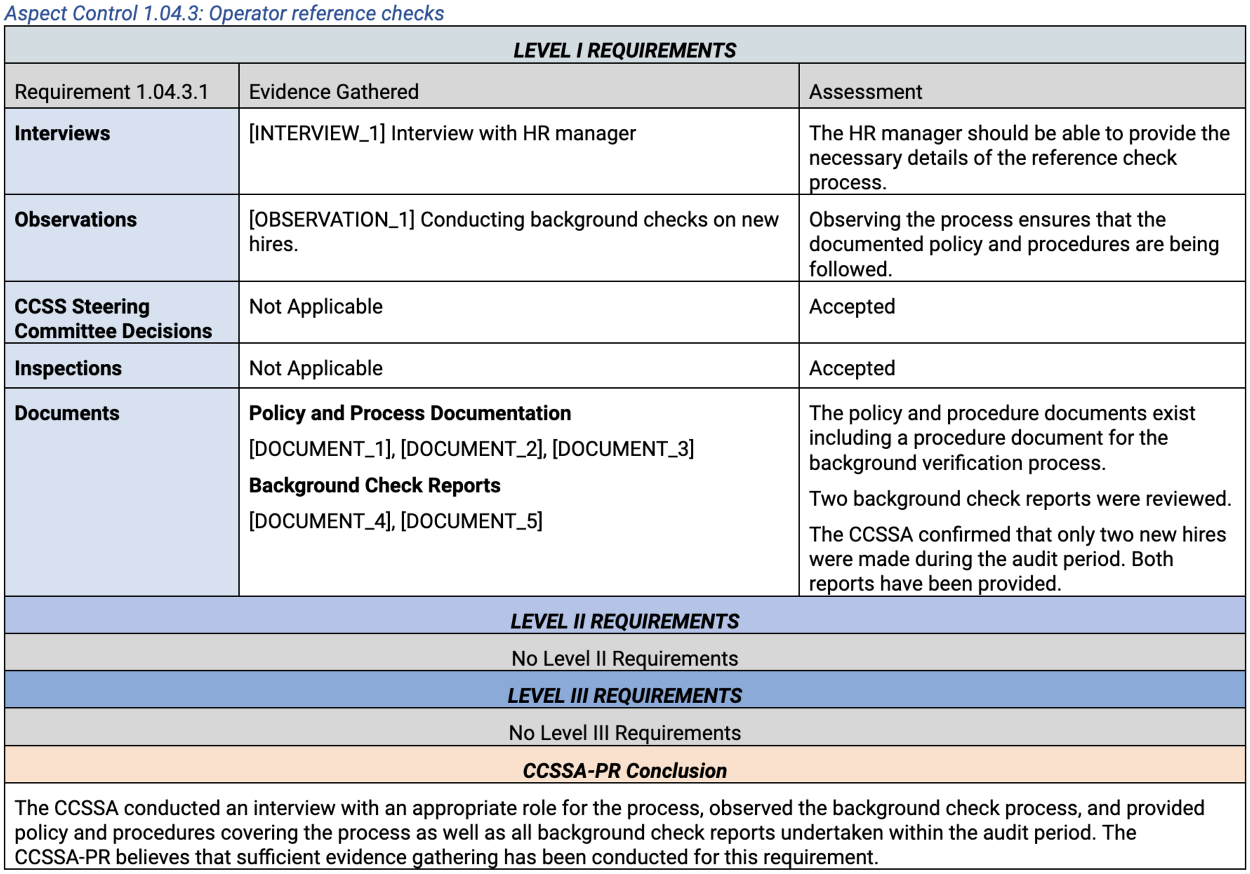


Aspect Control 1.04.3: Operator reference checks

LEVEL I REQUIREMENTS					
Requirement	1.04.3.1 All key/seed holders have had their references checked prior to being trusted to hold one of the organization's keys/seeds.				
Audit Finding Summary	**In-Place**	**In-Place with Comparable Control**	**Qualified for In-Place**	**Not In-Place**	**Not Applicable**
	☒	□	□	□	□
CCSSA Findings	The CCSSA reviewed the HR policy, which states that all candidates who will be offered a letter of employment must have a background check before the letter of employment is presented. The CCSSA reviewed the onboarding and background check process documents and confirmed that a background check process was documented. The CCSSA confirmed with the HR Manager that there were only two new hires within the audited period. The CCSSA reviewed the two background check reports and confirmed the at the background check reports were completed and reviewed by HR before each candidate was offered employment. The CCSSA reviewed the two candidates employment records and confirmed the date of the first day of employment was after the background check reports were sent to the HR manager, and both employment records recorded that the background check report had been reviewed with no issues reports in both reports. The CCSSA interviewed the HR manager, who confirmed that all candidates who will be offered a letter of employment have a background check undertaken by a third party before the letter of employment is offered.				
Evidence Gathered	*For each of the testing types below, provide information on the evidence gathered. If evidence of the type has not been gathered, indicate that next to the evidence type.*				

Figure 10 - Extract of Requirement 1.04.3.1 Findings Section in the Redacted ROC

Figure 10 shows that the CCSSA has amended the Redacted ROC requirement 1.04.3.1 findings section to state that only two new hires were made within the audit period.



Aspect Control 1.04.3: Operator reference checks

LEVEL I REQUIREMENTS		
Requirement 1.04.3.1	Evidence Gathered	Assessment
Interviews	[INTERVIEW_1] Interview with HR manager	The HR manager should be able to provide the necessary details of the reference check process.
Observations	[OBSERVATION_1] Conducting background checks on new hires.	Observing the process ensures that the documented policy and procedures are being followed.
CCSS Steering Committee Decisions	Not Applicable	Accepted
Inspections	Not Applicable	Accepted
Documents	**Policy and Process Documentation** [DOCUMENT_1], [DOCUMENT_2], [DOCUMENT_3] **Background Check Reports** [DOCUMENT_4], [DOCUMENT_5]	The policy and procedure documents exist including a procedure document for the background verification process. Two background check reports were reviewed. The CCSSA confirmed that only two new hires were made during the audit period. Both reports have been provided.
LEVEL II REQUIREMENTS		
No Level II Requirements		
LEVEL III REQUIREMENTS		
No Level III Requirements		
CCSSA-PR Conclusion		
The CCSSA conducted an interview with an appropriate role for the process, observed the background check process, and provided policy and procedures covering the process as well as all background check reports undertaken within the audit period. The CCSSA-PR believes that sufficient evidence gathering has been conducted for this requirement.		

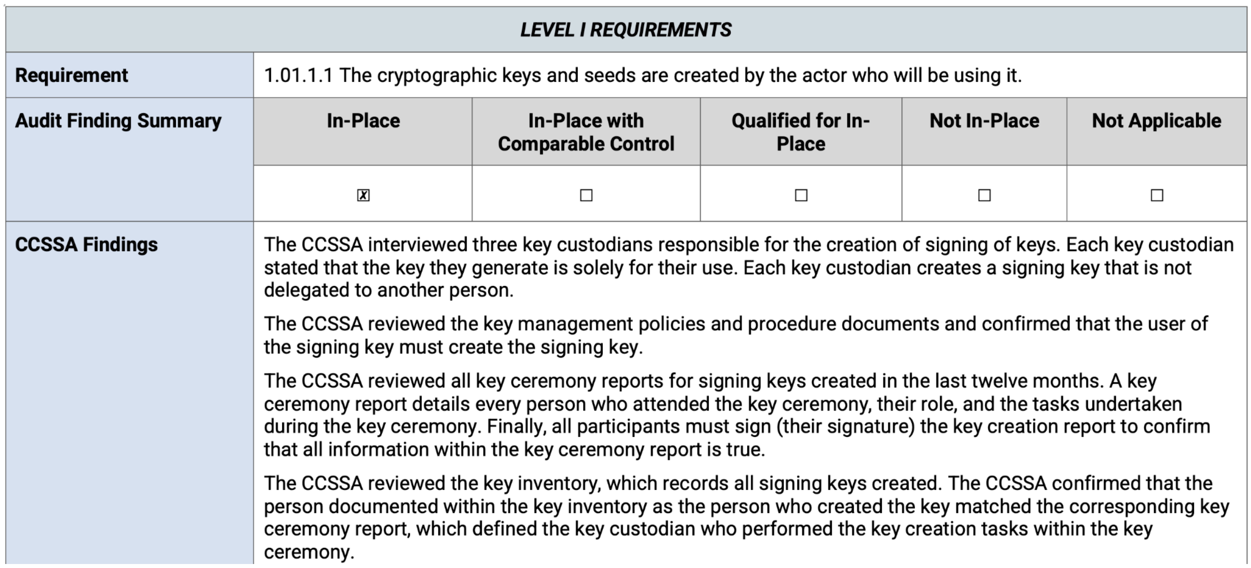
Figure 11 - Completed Peer Review for Requirement 1.04.3.1

Figure 11 shows the completed peer review findings for requirement 1.04.3.1. Note the “CCSSA-PR Conclusion” section at the bottom of the Aspect Control table.

Peer Review of Evidence Gathering Techniques

For each CCSS requirement, a section is provided in the Peer Review template that the CCSSA-PR must complete.

Here is an example below.



LEVEL I REQUIREMENTS					
Requirement	1.01.1.1 The cryptographic keys and seeds are created by the actor who will be using it.				
Audit Finding Summary	**In-Place**	**In-Place with Comparable Control**	**Qualified for In-Place**	**Not In-Place**	**Not Applicable**
	☒	□	□	□	□
CCSSA Findings	The CCSSA interviewed three key custodians responsible for the creation of signing of keys. Each key custodian stated that the key they generate is solely for their use. Each key custodian creates a signing key that is not delegated to another person. The CCSSA reviewed the key management policies and procedure documents and confirmed that the user of the signing key must create the signing key. The CCSSA reviewed all key ceremony reports for signing keys created in the last twelve months. A key ceremony report details every person who attended the key ceremony, their role, and the tasks undertaken during the key ceremony. Finally, all participants must sign (their signature) the key creation report to confirm that all information within the key ceremony report is true. The CCSSA reviewed the key inventory, which records all signing keys created. The CCSSA confirmed that the person documented within the key inventory as the person who created the key matched the corresponding key ceremony report, which defined the key custodian who performed the key creation tasks within the key ceremony.				

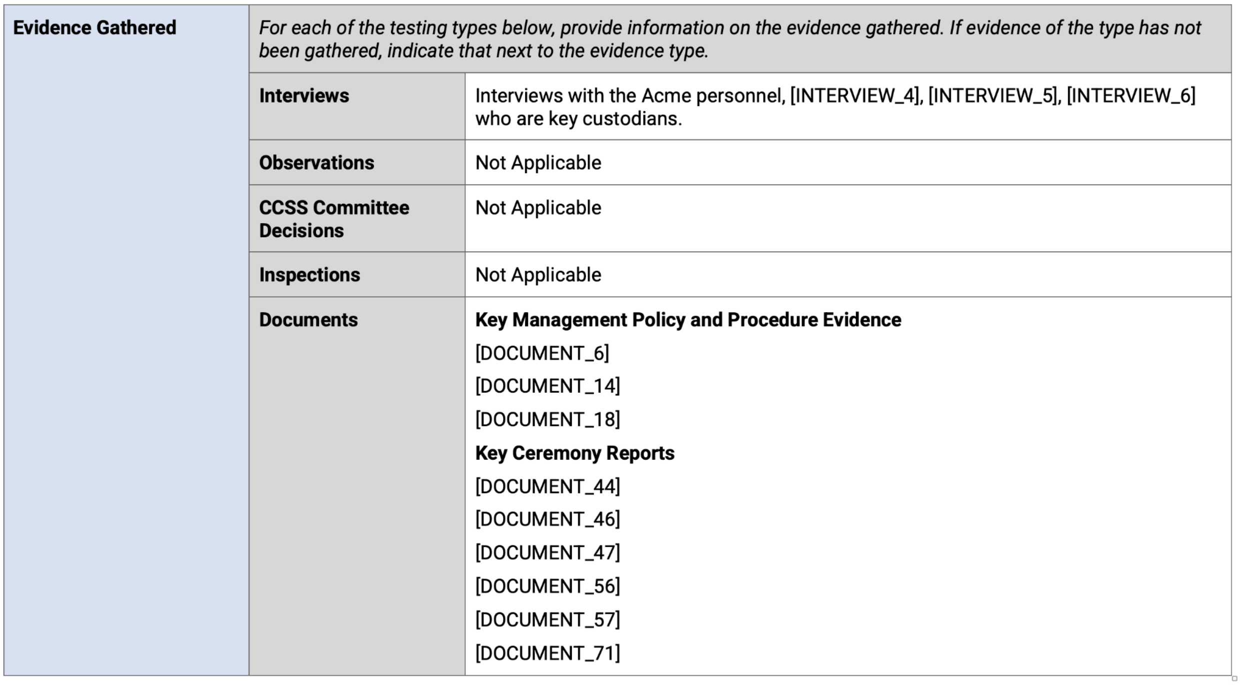
Figure 12 - An Example of a CCSS Redacted Report Requirement Section 1.01.1.1

Figure 12 is an example of a redacted RoC and the CCSS requirements findings section for requirement 1.01.1.1. The CCSSA has provided an overview of the findings gathered.

The example shows that the CCSSA used two evidence gathering techniques: (1) interview and (2) review.

In this example, the CCSSA-PR must determine if the evidence-gathering techniques used for this requirement are sufficient to meet the Audit Finding Summary, “In-Place.” The CCSSA-PR must also consider the evidence artifacts that CCSSA gathered.

The example continues below.



Evidence Gathered	*For each of the testing types below, provide information on the evidence gathered. If evidence of the type has not been gathered, indicate that next to the evidence type.*	
	Interviews	Interviews with the Acme personnel, [INTERVIEW_4], [INTERVIEW_5], [INTERVIEW_6] who are key custodians.
	Observations	Not Applicable
	CCSS Committee Decisions	Not Applicable
	Inspections	Not Applicable
	Documents	**Key Management Policy and Procedure Evidence** [DOCUMENT_6] [DOCUMENT_14] [DOCUMENT_18] **Key Ceremony Reports** [DOCUMENT_44] [DOCUMENT_46] [DOCUMENT_47] [DOCUMENT_56] [DOCUMENT_57] [DOCUMENT_71]

Figure 13 - The list of evidence artifacts gathered for requirement 1.01.1.1.

Figure 13 shows that the CCSSA reviewed the key management policies and procedures and reviewed key ceremony reports. The CCSSA also interviewed three key custodians.

For this example, the CCSSA-PR could consider when forming an opinion the following:

1. The CCSSA interviewed key custodians who are the actors as defined by CCSS. All of the interviewees confirmed that a user of a signing key must create the signing key. The signing key is not delegated.

2. The CCSSA confirmed that the statements made by the key custodians were correct by reviewing the key ceremony reports.

3. The CCSSA reviewed the key inventory, which the CCSSA probably considers a source of truth, that the key custodian recorded in the key inventory is the same person recorded in the relevant key ceremony report. These are two different sources of written information that confirm the key custodian's statements.

4. There are no observations recorded. However, it would not be prudent for a CCSSA to require a key ceremony to prove the statements made by the key custodians. In fact, the key ceremony would not prove anything. How can the key ceremony prove that the key

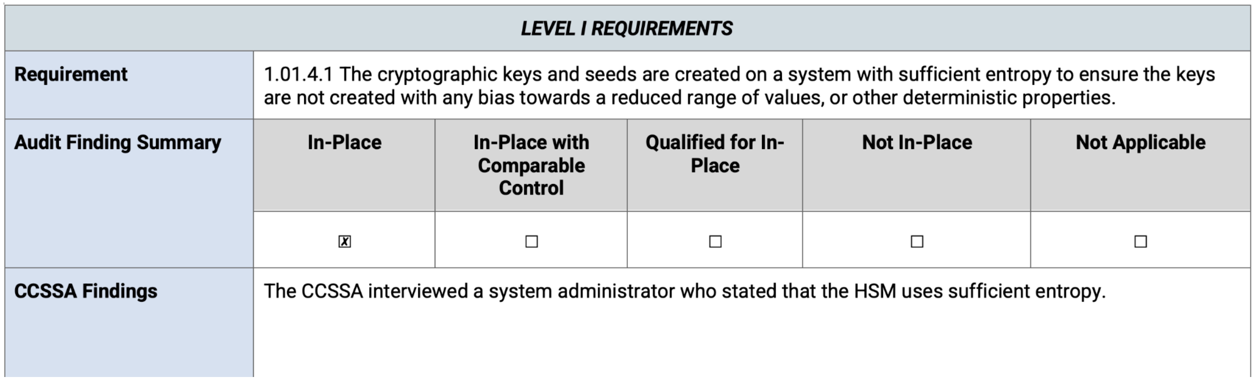
custodian who created the signing key is actually using it?

   a. NOTE: The entity may video record the key ceremony as part of its internal audit processes. In that case, the CCSSA could review the video to observe the key creation process.

5. There are no *CCSS Committee Decisions* related to this requirement. The key creation process appears quite normal, so there are no unusual processes where the CCSS Steering Committee would be required to provide a formal opinion.

6. No inspections are documented, which is acceptable for this requirement. For example, the HSM used during the key ceremony to create the signing key adds no proof of the intent of this requirement.

Another example is below.



LEVEL I REQUIREMENTS					
Requirement	1.01.4.1 The cryptographic keys and seeds are created on a system with sufficient entropy to ensure the keys are not created with any bias towards a reduced range of values, or other deterministic properties.				
Audit Finding Summary	**In-Place**	**In-Place with Comparable Control**	**Qualified for In-Place**	**Not In-Place**	**Not Applicable**
	☒	□	□	□	□
CCSSA Findings	The CCSSA interviewed a system administrator who stated that the HSM uses sufficient entropy.				

Figure 14 - An Example of a CCSS Redacted Report Requirement Section 1.01.4.1

Figure 14 is an example of a redacted RoC and the CCSS requirements findings section for requirement 1.01.4.1. The CCSSA has provided an overview of the findings gathered.

The example shows that the CCSSA used one evidence gathering technique: an interview.

The CCSSA-PR must determine if the evidence gathering techniques applied for this requirement are sufficient to meet the Audit Finding Summary, “In-Place”.

It is recommended that at least two evidence gathering techniques are used for every CCSS requirement. This example requirement would be suitable for at least three evidence gathering techniques.

For this example, conducting one interview is not enough evidence to have enough assurance that this requirement is “In-Place”. Consider the following points:

1. The CCSSA, in this example, states that a “system administrator” stated the HSM used sufficient entropy. The CCSSA does not state that the “system administrator” configures and maintains the HSM. The CCSSA might have interviewed a system administrator for desktop applications.

2. The CCSSA should have reviewed the policies, standards and procedure documents for configuring and maintaining the HSM to ensure that there are standards and configurations for the entropy mechanism.

3. The CCSSA should have inspected the HSM configurations to ensure the entropy mechanism was correctly configured based not only on the configuration standards and procedures of the entity but also on the HSM vendor's manual(s) to ensure that the entropy mechanism is configured correctly.

4. The CCSSA should have reviewed the third-party compliance certifications for the HSM to confirm that the entropy mechanism generates sufficient entropy.

5. The CCSSA must ensure that they interview personnel who configure the HSM and state the personnel's role to assure the CCSSA-PR that the correct person(s) was interviewed based on their role.

To further help the CCSSA and CCSSA-PR determine what evidence should be expected, the CCSS Advisory Group has provided a spreadsheet that lists the possible evidence types and evidence for each requirement. This spreadsheet is made available on the understanding that it is an informal guide. The spreadsheet **should not be** considered a mandatory list of evidence required for each requirement. You can find this document on C4’s CCSSA Resource Page.

Completing the Peer Review Process

The peer review process is officially complete when the CCSSA-PR puts in writing that the peer review process is complete. The official approval is documented in the section *Summary of Peer Review - CCSSA-PR Approval to Proceed to the Next Stage in the Audit* within the Peer Review Report.