CCSS Audit Methodology Handbook

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 goal of a CCSS audit is for an independent auditor (CCSSA) to conduct an audit on the information system(s) by collecting evidence that ensures appropriate information security controls have been implemented to meet the relevant CCSS requirements. The purpose of this handbook is to provide guidance to CCSS Auditors.

Audit Process

Audit Readiness Assessment

It is recommended that the CCSSA conducts an audit readiness assessment before the start of an official audit. An audit readiness assessment is a process where the CCSSA, with a fixed number of billable hours, conducts a high-level review of the people, processes, and technology components of the information system(s) to be audited in an attempt to be CCSS certified. The goal of the assessment is to identify if the information system (people, processes, and technology components) is ready for a CCSS audit. The output of the audit readiness assessment is a report much like a GAP assessment report outlining the missing components and suggested remediation activities.

For example, suppose the CCSSA, during the readiness assessment, identifies that there are no written policies or standards. In that case, this gap will impact the ability of the CCSSA to conduct an effective and efficient audit. Written policies, standards, and procedures are the cornerstone of any information system, and many CCSS requirements require documentation to exist.

If an audit readiness assessment was not undertaken before the official CCSS audit and the CCSSA only discovered the missing documentation during the audit, then this will dramatically impact the ability of the CCSSA to conduct the audit and, in fact, will likely pause the audit process until the required documentation is created. A pause to the audit will impact the timelines, including the time booked for the CCSSA-PR to peer review the redacted RoC.

Another well-known issue may arise when the audited entity asks the CCSSA to complete the documentation as part of the audit. This is a negative on at least two points: (1) the CCSSA did not factor into the hours quoted for the audit writing documentation for the entity, and (2) the CCSSA should not audit their own work. This is a well-known ethical principle for a professional auditor to eliminate potential bias in the audit findings.

An audit readiness assessment provides significant advantages to both the audited entity and the CCSSA. It enables the CCSSA to more precisely estimate the timeline for the official audit, as it identifies and addresses any factors that could affect the audit process during the assessment phase.

Initial Audit Considerations

For the initial CCSS audit, there are a few considerations that are applied that will not be applied in subsequent audits of the same information system. In this section, the considerations for the initial CCSS audit are covered.

Period Covered

A CCSS audit reviews the information systems, people, processes, and technology components from the twelve months preceding the audit start date. CCSS audit and certification is an annual process where the information system is audited every twelve months and upon a successful audit, CCSS certification is issued for another twelve months.

For the initial CCSS audit the information system may not have been in production for the full twelve months, which could result in evidence covering a shorter period than required. Consequently, the CCSSA must take this into account when evaluating the evidence and acknowledge that it may not cover the full twelve-month period. This is acceptable for the initial CCSS audit. The CCSSA must use their judgment to decide if the available evidence is sufficient to determine that a relevant requirement is "In-Place." They should not automatically conclude that a requirement is "Not In-Place" simply because the evidence does not span the full twelve months.

State of Documentation

One approach is for an initial audit to identify incomplete documentation such as policy/standard/procedure lacking the required statements, not kept up-to-date, or the documentation is nonexistent. Change management documentation may also be lacking.

For example, a cold wallet used by the in-scope system may have been created years ago and change management was not applied. This could mean key information is lacking, such as who created the wallet, who has access to the wallet, and where the wallet signing keys are located. The CCSSA, in this situation, may accept this finding only if change management is now implemented and any new wallets are created under change management.

Gathering Evidence

The goal of a CCSS audit is for an independent auditor (CCSSA) to conduct an audit on the information system(s) by collecting evidence that ensures appropriate information security controls have been implemented to meet the relevant CCSS requirements.

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

1. Review - reviewing documentation such as policy, standards, and procedures is the most common evidence-gathering technique. It 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.

   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 their control.

   a. A Policy is a document that defines the goals or "mission" of the entity, such as "*we provide a secure environment for our customers to transact.*"
   b. A Standard is a document that will outline the best practices, based on internationally recognized standards, as to how the entity will meet this goal, such as "*the entity implements strong access control mechanisms that conform to ISO27001 or NIST 800-53*" and another example "*the entity uses an HSM certified to FIPS 140-3.*"
   c. A Procedure is a document that defines exactly how a goal is to be achieved. A procedure document will list the steps or tasks involved to achieve a result. For example, a procedure document can be used to onboard a new customer or configure a new HSM.

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 deviating from these. Deviations 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 their 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 a specific action has been taken, 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.”

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.

Review the section *Recommendations for Completing the Detailed Findings Section* in this guidance document for a detailed overview of how evidence can be reported within the RoC.

Audit Regulations

1. The CCSSA cannot accept anything that does not exist as evidence. For example, the entity might state to the CCSSA that the current CCSS non-compliant mechanism that generates entropy will be replaced soon with a CCSS-supported entropy mechanism. This is considered “future-dated” and unacceptable evidence for a CCSS audit.
2. CCSS requirements cannot be changed, removed, or additional requirements added for a CCSS audit. The only organization that can change the CCSS requirements is the CCSS Steering Committee.
3. The official C4 documentation for an audit (RoC, SRoC, Intent to Audit, Appendix 1) cannot be altered, such as changes to wording, formatting, or branding without written approval from the CCSS Steering Committee.

Seeking Opinion or Help from the CCSS Steering Committee

During an audit, the CCSSA may find systems that have been configured or implemented that do not fit the exact wording of a CCSS requirement.

For example, CCSS requirements refer to multiple “keys" used for signing a transaction. If a system uses an implementation of Multi-Party Computation (MPC) where one signing key is split or sharded into many parts and each “shard” is used to sign a transaction, then could a “shard” be considered a “key” to meet relevant CCSS requirements? This is an example of a question that could be submitted to the CCSS Steering Committee for consideration. The CCSS Steering Committee can then provide an opinion on whether an MPC “shard” is considered a signing key or not.

The CCSSA needs to include their name, auditor ID#, the requirement in question, and information about the situation that brings that requirement into question. Also include whether or not this pertains to an ongoing audit. No proprietary or sensitive information about the entity or system being audited should be included.
For questions regarding ongoing audits, the committee shall review the evidence and provide a decision within 15 business days.

Documentation for the questioned requirement should be submitted to the committee at CCSS_Submissions@cryptoconsortium.org

Audit Documentation

Report on Compliance (RoC)

Benefits

The CCSSA must use the official C4 Report on Compliance (RoC) template document to record the audit findings. Using the C4 official RoC to record audit findings has several benefits to all entities involved in a CCSS audit:

1. Provides consistency and accuracy in documenting audit findings by ensuring that no required audit information is missed in the audit process.

2. Provides accuracy for the CCSSA-PR, who has to provide a quote for the peer review process on the understanding that the CCSSA will use the official RoC template.

3. Provides a reliable expectation by the audited entity that the audit report will be consistent even if a different CCSSA is used for each audit.

4. Provides assurance to C4 and the CCSS Steering Committee that all CCSSAs follow the CCSS audit process, including applying the required evidence-gathering techniques, how the status of a requirement finding was determined, and documenting the findings.

C4 Official RoC is Mandatory for CCSS Audits

The C4 official RoC is required to report all CCSS audits. If a CCSSA does not use the C4 official RoC, the CCSSA-PR must reject the audit report.

C4 Official RoC Location

The C4 official RoC template can be downloaded from the CCSSA Resources Portal. For each CCSS audit, the CCSSA should check for the latest version of the RoC template by downloading a fresh copy from the CCSSA Resources Portal.

CCSS is frequently updated; therefore, the RoC template may be updated to reflect changes to CCSS or an audit-related process.

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

RoC Sections

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

RoC Section	Section Purpose
Document Template History and Version History	This section records the current template version and previous versions.
About the CryptoCurrency Security Standard (CCSS)	This section provides an overview of the CryptoCurrency Security Standard (CCSS) and the CCSS audit and certification process.
Audit Finding Statuses	This section defines the audit findings status that are supported in CCSS. Refer to this guidance's section *Audit Finding Statuses,* for a detailed description.
Contact Information	This section records the details of the audited entity, the CCSSA and the CCSSA-PR. These sections must be completed. Note: An entity cannot be anonymous. The CCSS audit and certification processes provide assurance and accountability of information systems information security controls.
Summary of Audit	This section defines the following: ● The audit testing period is the start and end of the audit process. The end is when evidence collection has been completed. ● The Demonstrated CCSS Level is the CCSS Level that audited systems have reached based on the evidence collected during the audit by the CCSSA and reviewed by the CCSSA-PR. ● CCSSA Explanation of CCSS Level Achieved requires that the CCSSA documents at a high level the roles, processes, and technology components that were interviewed, inspected and reviewed to determine the CCSS Level obtained. ● The CCSSA reports the CCSS Level obtained in the CCSS aspect table. The determination of the overall CCSS Level for an information system applies the principle of the weakest link. For detailed information, refer to *Appendix A - CCSS Compliance Levels* in this guidance.

CCSS Trusted Environment Summary - Trusted Environment	This section defines the CCSS Trusted Environment, which consists of the people, processes, and technology components of the information system(s) audited for compliance with CCSS.
CCSS Trusted Environment Summary - Validation of Trusted Environment	This section defines how the CCSS scope was validated. It is the responsibility of the audited entity to define the scope of the information system(s) that are to be audited for CCSS certification. The CCSSA must validate the defined scope to ensure all components (people, processes, and technology) have been identified.
Evidence Retention	This section records who (CCSSA or entity under audit) will be responsible for storing the audit evidence collected during the audit. The legal jurisdiction of the entity stipulates the retention period.
Detailed Findings	This section lists all CCSS requirements. For each requirement, an evidence table is provided. Refer to the “Structure of Detailed Findings” section within this chapter for a detailed overview of the evidence table.
Audit Evidence Interviews Conducted Documentation Reviewed Process Observations Inspections CCSS Committee Decisions	This section provides tables covering each evidence-gathering technique applied during the audit. For example, the “Interviews Conducted” records all personnel interviewed and the topics covered in each interview. The “Documentation Reviewed” records all documentation reviewed by the CCSSA during the audit. “Process Observations” record which processes were observed and the determination of if those processes match procedures stated in the standards and policy documentation. “Inspections” record which system configurations and other technology components were inspected and whether those systems and components meet requirements stated in the standards and policy documentation. The “CCSS Committee Decisions” records any decisions made by the CCSS Steering Committee in response to a request for clarification from the CCSSA conducting the audit. For example, the CCSSA may seek a decision from the CCSS Steering Committee regarding the suitability of an information security control implemented for a particular CCSS requirement and

	whether the control meets the intent of a requirement.

CCSS Trusted Environment Definition

As with any audit, identifying the audit scope is the most important step as the scope definition places a boundary around the people, processes, and technology components to be included in the CCSS audit and avoids including components that are not needed. Not identifying the scope before the audit could result in extra effort, time, and cost during the audit as the CCSSA will be forced to define the scope, which is not ideal.

It is the responsibility of the audited entity to define the CCSS Trusted Environment. The role of the CCSSA during the audit process is to verify the accuracy of the CCSS Trusted Environment to ensure all people, processes and technology components that are key management systems and any other components that could impact the security of the key management systems have been included in the audit scope.

For example, an HSM that stores the keys used for signing transactions is in the CCSS audit scope. The personnel who have access to the HSM are also in the CCSS audit scope, as are the policy and procedures for managing the HSM.

But also consider that if the HSM is a cloud service such as AWS KMS, the AWS access controls that provide access to the KMS services are also in CCSS audit scope because the access controls could impact the security of the KMS service that hosts the keys. If the access controls are not configured correctly to allow only roles that need access to configure the KMS service, such as HSM administrators, for example, marketing personnel could access the KMS service. The security of the keys could be impacted via a weak access control policy.

The CCSSA should validate the Trusted Environment scope in the following ways:

1. Review all network diagrams and business component flow diagrams.
2. Review all high level and detailed design architectural documents for the components.
3. Interview all relevant roles as sometimes “shadow IT” can be located via interviews.
4. Review all policy, standards and procedure documents.
5. Review all third-party certification reports such as for ISO27001 and SOC 2.
6. Review the public website and help guides.

7. Inspect the software and systems configurations, not only the key management systems, but the systems provided to the customer.

8. Review the security controls such as access controls, firewalls, IDS/IPS, anti-malware systems etc..

9. Review BAU reports, such as change tickets, pen-testing reports, internal assessment reports, vulnerability scan reports, patching tickets, incident response reports, and access management reports (e.g., interactive user account reports).

10. Identify any service providers in-scope such as managed security operation services, wallet infrastructure services etc..

Structure Of Detailed Findings Section

Figure 2 below provides an extract of a CCSS requirement evidence collection table from the CCSS RoC template.

Aspect Control 1.02.3: Geographic distribution of keys

LEVEL I REQUIREMENTS					
No Level I Requirements					
LEVEL II REQUIREMENTS					
Requirement	1.02.3.1 Any keys that have signing authority on a single wallet must be stored in different locations.				
Audit Finding Summary	**In-Place**	**In-Place with Comparable Control**	**Qualified for In-Place**	**Not In-Place**	**Not Applicable**
	☐	☐	☐	☐	☐
CCSSA Findings					
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				
	Observations				
	CCSS Committee Decisions				
	Inspections				
	Documents				

Figure 2 - An Example of a CCSS requirement evidence collection table from the CCSS RoC template.

The first few rows of the evidence collection table define to which CCSS Level the requirement belongs. We can see that the requirement belongs to CCSS Level 2.

The next row, “Requirement” defines the CCSS requirement for this evidence collection table, which, for our example extract, is requirement 1.02.3.1.

The next row, “Audit Finding Summary,” records the CCSSA's findings status for the requirement. Five findings statuses are currently defined for CCSS. The CCSSA checks the checkbox for the findings status identified for the requirement. Refer to the section *Audit Finding Statuses* within this guidance for an overview of each of the findings statuses.

The next row, “CCSSA Findings”, is where the CCSSA records the findings based on the evidence gathered for this requirement.

In the final row, “Evidence Gathered,” the CCSSA records all the evidence gathered and reviewed/inspected/observed. Any CCSS Steering Committee decisions for this requirement are recorded in the “CCSS Committee Decisions” section along with the date the decision was emailed to the CCSSA.

Recommendations for Completing the Detailed Findings Section

There is no mandatory approach to recording evidence in the detailed findings section of the RoC. However, this guidance recommends an approach so the CCSSA can take advantage of the RoC's structure to reduce the effort and time spent completing the detailed findings section. The examples also show the level of detail required to provide evidence that a CCSSA had enough evidence to form the opinion for each CCSS requirement.

The CCSSA Findings section is where the CCSSA adds in what was identified and confirmed from the collection of evidence for a requirement. Continuing with the two examples above.

Example One - Requirement 1.04.3.1 Reporting

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.

The CCSSA collected the following evidence, which is defined in the table below.

Type of Evidence	Evidence
Reviewed policies and/or standards that require all personnel with access to a signing key to have a reference check undertaken before access is granted.	HR Onboarding Process.pdf HR Background Verification Process.pdf HR Policy.pdf
Interviewed relevant personnel who are responsible for ensuring a reference check is undertaken.	Interviewed Joe Bloggs, who is the HR Manager, about the background checks process.
Observed the process of conducting a reference check.	Observed Joe Bloggs demonstrating to the CCSSA how the background check report is requested from the third party that conducts the background checks.
Reviewed a sample of reference check reports.	Reviewed background checks for Jane Doe and John Smith. Jane Doe Background Check Report 21-Mar-2024.pdf John Smith Background Check Report 01-Sept-2024.pdf

Now that evidence has been collected, the CCSSA will add the evidence to the relevant section in the Audit Evidence section at the end of the RoC template.

Documentation Reviewed [DOCUMENT]

Reference Number	Document Name	Description of Document Purpose	Document Revision Date (if applicable)
DOCUMENT_1	HR Onboarding Process.pdf	Defines the onboarding process for all new personnel who joined the organization.	01-Jan-2024
DOCUMENT_2	HR Background Verification Process.pdf	Provides detailed steps to conduct a background check that the HR department must perform for all new hires.	01-Jan-2024
DOCUMENT_3	HR Policy.pdf	The overall HR policy defines the mission and goals of the HR department. The policy states that the HR department must undertake a background check on a selected candidate before a letter of offer is provided to the candidate selected for hire.	01-Jan-2024
DOCUMENT_4	Jane Doe Background Check Report 21-Mar-2024.pdf	Background check report for a new hire. The report contains findings on reference, previous employment, identification and crimal checks.	Not Applicable
DOCUMENT_5	John Smith Background Check Report 01-Sept-2024.pdf	Background check report for a new hire. The report contains findings on reference, previous employment, identification and crimal checks.	Not Applicable

Figure 3 - The example documented evidence recorded in the Documentation Reviewed evidence table.

The documented evidence has been added to the *Documentation Reviewed* evidence table. Note that the *Reference Number* column is a *DOCUMENT_* tag with a sequential number that can reference documented evidence in the RoC.

Interviews Conducted [INTERVIEW]

Reference Number	Topics Covered in Interviews	Interviewee Name	Interviewee Role	Interviewee Organization
INTERVIEW_1	The background check process for new hires, onboarding and offboarding processes.	Joe Bloggs	HR Manager	ACME

Figure 4 - The example interview recorded in the Interviews Conducted evidence table.

The interview with the HR manager has been added to the *Interviews Conducted* evidence table. Note that the *Reference Number* column is an *INTERVIEW_* tag with a sequential number that can reference the interview evidence in the RoC.

Process Observations [OBSERVATION]

Reference Number	Process Observed	Description of What Was Observed	Date Observed
OBSERVATION_1	Conducting background checks on new hires.	Observed Joe Bloggs demonstrating to the CCSSA how the background check report is requested from the third party that conducts the background checks.	15-Dec-2024

Figure 5 - The example observation recorded in the Process Observations evidence table.

The observation of the process of conducting a background check on a new hire has been added to the *Process Observations* evidence table.

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					
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.			
	CCSS Committee Decisions	Not Applicable			
	Inspections	Not Applicable			
	Documents	**Policy and Process Documentation** [DOCUMENT_1], [DOCUMENT_2], [DOCUMENT_3] **Background Check Reports** [DOCUMENT_4], [DOCUMENT_5]			
LEVEL II REQUIREMENTS					

Figure 6 - Evidence reference tags have been added to requirement 1.04.3.1

Figure 6 shows the Evidence Gathered section for requirement 1.04.3.1 completed. The evidence-gathering techniques not used for requirement 1.0.4.3.1 are marked as *Not Applicable* to ensure the reader (including the CCSSA-PR) does not believe evidence is missing.

Figure 6 shows the benefit of using evidence reference tags because if the CCSSA receives an updated HR policy document where the file name has changed, the CCSSA just needs to update the file name in the Document Reviewed section. Further, when redacting the RoC for the CCSSA-PR, the redaction of the file name will probably be required. This saves time and effort for the CCSSA-PR in reviewing the redacted RoC.

Now that the evidence gathered has been added to the *Evidence Gathered* section of requirement 1.04.3.1, the CCSSA can complete the *CCSSA Findings* section of requirement 1.04.3.1 referencing the evidence documented.

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 7 - The CCSSA Findings section has been completed.

Figure 7 shows the *CCSSA Findings* section completed by the CCSSA. The findings documented by the CCSSA reference the evidence recorded in the *Evidence Gathered* section of the requirement.

Based on the evidence gathered, the CCSSA forms an opinion that requirement 1.04.3.1 is met, and therefore, the Audit Finding Summary can be completed by checking the *In-Place* findings status (Figure 8).

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 - The CCSSA checks the *In-Place* findings status.

Once the CCSSA checks the In-Place findings status for requirement 1.04.3.1 this requirement is complete and the CCSSA can move on to another requirement.

Example Two - Requirement 1.01.4.1 Reporting

> *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.*

The CCSSA collected the following evidence, which is defined in the table below.

Type of Evidence	Evidence
Reviewed policies and/or standards that require mechanisms that generate entropy to be sufficient for CCSS.	Key management policy.pdf Key generation process.pdf Cryptographic standard.pdf
Interviewed relevant personnel who are responsible for ensuring a reference check is undertaken.	Interviewed Mary Bloggs, HSM systems administrator, about the HSM configuration. Interviewed Jim Bloggs, cryptographic architect, about the key generation process.
Inspected HSM configuration, including entropy settings.	HSM configuration screen captures.
Reviewed HSM vendor certifications.	FIPS 140-3 Level 3 Certified Luna HSM Firmware Versions. https://thalesdocs.com/gphsm/luna/7/docs/pci/Content/compliance/fips.htm Thales Cryptovisor K7 Cryptographic Module Level 3 Non-Proprietary Policy compliance with CCSS applicable requirements.

Now that evidence has been collected, the CCSSA will add the evidence to the relevant section in the Audit Evidence section at the end of the RoC template.

Reference Number	Document Name	Description of Document Purpose	Document Revision Date (if applicable)
DOCUMENT_6	Key management policy.pdf	High-level key management policy defining the key management processes for the entire key management life-cycle.	01-Feb-2024
DOCUMENT_7	Key generation proces.pdf	Documented key generation process defining all tasks, including roles and responsibilities when generating a signing key.	01-Feb-2024
DOCUMENT_8	Cryptographic standard.pdf	Standard defining the supported cryptographic key strengths and ciphers used within the organization.	01-Feb-2024
DOCUMENT_9	Thales Luna FIPS 140-3 offical information.	FIPS 140-3 Level 3 Certified Thales Luna HSM Firmware Versions https://thalesdocs.com/gphsm/luna/7/docs/pci/Content/compliance/fips.htm	Not Applicable
DOCUMENT_10	140sp4327.pdf	Thales Cryptovisor K7 Cryptographic Module Level 3 Non-Proprietary Policy compliance with CCSS applicable requirements.	12-Nov-2023

Figure 9 - The example documented evidence recorded in the Documentation Reviewed evidence table for CCSS requirement.

Interviews Conducted [INTERVIEW]

Reference Number	Topics Covered in Interviews	Interviewee Name	Interviewee Role	Interviewee Organization
INTERVIEW_1	The background check process for new hires, onboarding and offboarding processes.	Joe Bloggs	HR Manager	ACME
INTERVIEW_2	Dicussion on the overview of the Thales Luna HSM which generates keys. Inspected the HSM configuration has part of the interview.	Mary Bloggs	HSM Systems Administrator	ACME
INTERVIEW_3	Dicussion on the key generation process including interactions with HSM during the process.	Jim Bloggs	Cryptographic Architect	ACME

Figure 10 - Two interviewees added to the Interviews Conducted evidence table.

Two interviews were conducted for this requirement and added to the *Interviews Conducted* evidence table.

Inspections [INSPECTION]

Reference Number	What Was Inspected	Inspection Findings	Date Inspected
INSPECTION_1	Thales Luna HSM configuration.	The CCSSA inspected Thales Luna's HSM configuration, and it was confirmed that there was no ability to change the entropy configurations.	16-Dec-2024

Figure 11 - The Thales Luna HSM configuration inspection is recorded in the Inspections evidence table.

The inspection of Thales Luna HSM configuration was undertaken by the CCSSA during an interview and recorded in the *Inspections* evidence table

Aspect Control 1.01.4: Entropy Pool

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					
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_2] Inspected the HSM configuration has part of the interview. [INTERVIEW_3] Dicussion on the key generation process including interactions with HSM during the process.			
	Observations	Not Applicable			
	CCSS Committee Decisions	Not Applicable			
	Inspections	[INSPECTION_1] Thales Luna HSM configuration.			
	Documents	**Key Management Policy and Standards** [DOCUMENT_6], [DOCUMENT_7], [DOCUMENT_8] **HSM FIPS Certification** [DOCUMENT_9]			

Figure 12 - Evidence reference tags have been added to requirement 1.01.4.1

Figure 12 shows the Evidence Gathered section for requirement 1.01.4.1 completed. The evidence-gathering techniques not used for requirement 1.01.4.1 are marked as *Not Applicable* to ensure the reader (including the CCSSA-PR) does not think any evidence is missing.

Aspect Control 1.01.4: Entropy Pool

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	Thales Luna HSM is a cloud-based HSM service provided by Thales. The Thales Luna HSM cryptovisior K7 cryptographic module is certified FIPS 140-3. The CCSSA confirmed the FIPS 140-3 certification by reviewing the Thales Luna FIPS 140-3 Non-Proprietary Security Policy. On page 46 of the Non-Proprietary Security Policy, the "Random Number Generation" section defines the entropy algorithm as "ENT (P)" and conforms to NIST SP800-90 which is required by CCSS.				
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_2] Inspected the HSM configuration has part of the interview. [INTERVIEW_3] Dicussion on the key generation process including interactions with HSM during the process.			
	Observations	Not Applicable			
	CCSS Committee Decisions	Not Applicable			
	Inspections	[INSPECTION_1] Thales Luna HSM configuration.			
	Documents	**Key Management Policy and Standards**			

Figure 13 - The CCSSA Findings section has been completed.

Figure 13 shows the *CCSSA Findings* section completed by the CCSSA. The findings documented by the CCSSA reference the evidence recorded in the *Evidence Gathered* section of the requirement.

Aspect Control 1.01.4: Entropy Pool

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	Thales Luna HSM is a cloud-based HSM service provided by Thales. The Thales Luna HSM cryptovisior K7 cryptographic module is certified FIPS 140-3. The CCSSA confirmed the FIPS 140-3 certification by reviewing the Thales Luna FIPS 140-3 Non-Proprietary Security Policy. On page 46 of the Non-Proprietary Security Policy, the "Random Number Generation" section defines the entropy algorithm as "ENT (P)" and conforms to NIST SP800-90 which is required by CCSS.				
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_2] Inspected the HSM configuration has part of the interview. [INTERVIEW_3] Dicussion on the key generation process including interactions with HSM during the process.			
	Observations	Not Applicable			
	CCSS Committee Decisions	Not Applicable			
	Inspections	[INSPECTION_1] Thales Luna HSM configuration.			
	Documents	**Key Management Policy and Standards**			

Figure 14 - The CCSSA checks the *In-Place* findings status.

Based on the evidence gathered, the CCSSA forms an opinion that requirement 1.01.4.1 is met, and therefore, the Audit Finding Summary can be completed by checking the *In-Place* findings status (Figure 14).

Example of An Unacceptable Requirement Section

The reporting examples above show the level of detail required for a CCSSA to document the facts identified by the review of evidence gathered. If the evidence gathered for this requirement is sufficient, then the CCSSA should be able to form an opinion as to the findings status of the requirement. This is important for the peer review process and for ensuring that the integrity of the CCSS audit and certification process remains high.

This section defines what is unacceptable regarding documentation of a requirement within the RoC.

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	Yes, all key/seed holders have had their references checked prior to being trusted to hold one of the organization's keys/seeds.				
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	HR manger			
	Observations				
	CCSS Committee Decisions				
	Inspections				
	Documents	Policy and other doco.			
LEVEL II REQUIREMENTS					
No Level II Requirements					

Figure 15 - Example of unacceptable reporting.

Figure 15 shows an example of unacceptable reporting for a requirement. The CCSSA has provided, "*Yes, all key/seed holders have had their references checked prior to being trusted to hold one of the entity's keys/seeds.*"

The statement is insufficient to prove to the CCSSA-PR that enough evidence was gathered so that the CCSSA can form a valid opinion if the requirement's intent has been met. The CCSSA has also parroted the requirement in the statement without detailing the facts identified based on the evidence gathered.

The CCSSA has also provided insufficient documentation of the evidence gathered.

The example shows that for interviews, the CCSSA added "*HR manager*" but did not provide details on the interview topics, so the CCSSA-PR would not know if the interview included a discussion on the background check process.

The CCSSA added "*Policy and other doco*" in the *Documents* section, which is insufficient. The CCSSA did not include any details on what policy was reviewed and other documentation and whether it was relevant to this requirement.

The CCSSA did not add “Not Applicable” to the other evidence sections, so the CCSSA-PR will not know if the CCSSA completed the requirement or if the CCSSA forgot to complete the requirements evidence sections.

This example would fail the peer review based on the requirements defined in the Peer Review Guidance document, which is located on C4’s CCSSA Resource Page.

Redacted Report on Compliance (Redacted RoC)

C4 and the CCSS Steering Committee require that the peer review process for a RoC be conducted by another CCSSA who does not have a previous or existing relationship with the CCSSA that performed the audit or the entity under audit. For example, a CCSSA employed or contracted with the same organization as the CCSSA that conducted the peer review cannot undertake the peer review process.

Once the CCSSA has completed the RoC, the next stage of the CCSS audit process is to redact it so it is ready for peer review. The redaction process ensures that all confidential information and personally identifiable information (PII) are removed from the RoC before the CCSSA-PR can review it.

The CCSSA who conducted the audit must make a copy of the RoC and, with that copy, redact all confidential information and PII from that copy. The redacted RoC is the version of the RoC that the CCSSA-PR peer reviews. The redaction process undertaken by the CCSSA should include a review of the redacted RoC by the audited entity to ensure that no confidential information is present within the redacted RoC. Once the audited entity has reviewed the redacted RoC then approval can be given, in writing, by the audited entity to release the redacted RoC to the CCSSA-PR who will use the redacted RoC to complete the Peer Review Report.

Once the peer review is completed, the CCSSA-PR will submit any queries to the CCSSA, and the CCSSA will have the opportunity to respond to them.

Note that the peer review process may involve remediation of the RoC due to feedback provided by the CCSSA-PR. Any remediation undertaken by the CCSSA due to CCSSA-PR feedback must be reviewed by the CCSSA-PR and confirmed as completed.

The CCSSA-PR must provide written confirmation to the CCSSA that the peer review process is complete and no further remediation is required so that the CCSSA can continue with the audit process.

Summary Report on Compliance (SRoC)

The SRoC is an official C4 document that the CCSSA completes at the end of the audit. The SRoC captures the following details:

1. Entity name
2. CCSS version audited under
3. Date of SRoC creation
4. Information system(s) audited
5. CCSS system designation
6. CCSS Compliance Level obtained
7. Description of systems (high-level overview of the information systems audited)
8. Description of environment (high-level overview of the CCSS Trusted Environment)
9. CCSSA name and CCSSA certification ID
10. CCSSA-PR name and CCSSA-PR certification ID

Once the audit has been completed and the audited entity is ready for the CCSS certification process, the SRoC is sent to CCSS_Submissions@cryptoconsortium.org and cc'ing the CCSSA-PR. The SRoC will not contain any PII or sensitive information regarding the information system(s) audited.

The SRoC can be compared to the PCI DSS Attestation of Compliance (AOC) document, which is where entities seek information about the scope and compliance of the entity's CCSS-certified information system(s). The entity that has the CCSS-certified systems is the only entity that can distribute its SRoC. The CCSSA and C4 will not disclose the SRoC to any organization. Normally, the SRoC is provided to an organization under NDA. The SRoC is not provided to the CCSSA-PR for peer review as the SRoC is only created once the redacted RoC passes the peer review process.

Appendices

Appendix A - CCSS Compliance Levels

C4 has incorporated into the CCSS certification program a unique approach to gaining CCSS certification by implementing three levels for CCSS compliance. Each CCSS compliance “Level” represents how many of the CCSS requirements the information system has implemented.

There are three CCSS Levels: Level 1, Level 2, and Level 3, which are explained below.

The CCSS Level system starts with Level 1 under which the baseline controls are required to be implemented. This is the minimal level of CCSS certification.

CCSS Level 2 adds further information security controls in addition to the controls required in CCSS Level 1.

CCSS Level 3 is the highest level currently and adds further information security controls in addition to the information security controls implemented at CCSS Levels 1 and 2.

Each Aspect Control defines requirements that can be CCSS Level 1, 2 or 3.

For example, 2.01.1 Security Audit defines the following requirements:

CCSS Level 1
2.01.1.1 A developer who is knowledgeable about digital asset security has assisted in the design and implementation of the information system and documentation of an internal assessment exists.

CCSS Level 2
2.01.1.2 A regular security assessment that includes vulnerability and penetration testing has been completed by an independent qualified third party. Documentation shows that all concerns raised by the assessment have been evaluated for risk and addressed by the entity.

CCSS Level 3
2.01.1.3 A regular security audit at a level similar to SOC2, ISAE3402, or ISO-27001, which includes vulnerability, penetration testing, and code audit (if applicable), and that has been completed by an independent qualified third party. Documentation shows that all concerns raised by the audit have been evaluated for risk, addressed by the entity, and known vulnerabilities have been removed from the system. Ongoing audits are scheduled on a (minimum) yearly basis.

As you can see with our example requirement, the amount and complexity of information security controls required to meet the intent of the requirement increases with each level.

An information system can be certified overall at CCSS Levels 1, 2 or 3. To reach CCSS Level 1 overall certification the information system needs to meet all requirements within all applicable Aspect Controls for level 1. To reach CCSS Level 2 overall certification the information system needs to meet all requirements within all applicable Aspect Controls for levels 1 and 2. To reach CCSS Level 3 overall certification the information system needs to meet all requirements within all applicable Aspect Controls for levels 1, 2, and 3.

Appendix B - Audit Finding Statuses

The CCSSA must provide a findings status for each CCSS requirement based on the evidence collected during the audit. In addition to applying a findings status for each CCSS requirement, the CCSSA must also provide an overall findings status for each CCSS Aspect.

Finding Status	Definition
In-Place	All parts of the demonstrated process were shown to meet the requirement as written in the CCSS.
In-Place with Comparable Control	A control is implemented by the entity that provides equivalent or comparable protection to the control defined in the CCSS.
Qualified for In-Place	All parts of the demonstrated process within the information system's control were shown to meet the requirement as written in the CCSS. However, some elements lay beyond the audited information system's control. When a CCSS requirement has been identified as "Qualified for In-Place" the information system will likely be designated as a QSP. For example, if the audited information system only controls some of the signing keys used for a transaction and the remaining signing keys are controlled by the customer, then the audited entity cannot be expected to be audited on the customer's systems which control the customers signing keys they are responsible for. Therefore, the audited entity's systems are only audited. This means that relevant CCSS requirements are not fully "In-Place" because the customer's systems had not been audited in this audit and, therefore, meets the "Qualified for In-Place" status.

Not In-Place	One or more parts of the demonstrated processes did not meet the requirement as written in the CCSS and no comparable control was provided.
Not Applicable	This indicates that the requirement does not apply to the entity's environment, and it has been evidenced by the CCSSA that the entity's environment does not support or provide a facility that would meet the requirement's intent when marking the control as not applicable. This findings status can also be applied to CCSS requirements that belong to a CCSS Compliance Level that the entity is not seeking. For example, if the entity is only requiring CCSS Compliance Level 2 then all CCSS Compliance Level 3 requirements would be marked as Not Applicable.