CryptoCurrency Security Standard Auditor (CCSSA) Guide

[CryptoCurrency Security Standard Auditor (CCSSA) Guide](#)

[1. Audit Process](#)
- [1.1 Appointment](#)
  - [1.1.1 Agreement](#)
  - [1.1.2 Fees](#)
    - [1.1.2.1 Audit Fees](#)
    - [1.1.2.2 Listing Fee](#)
  - [1.1.3 Confidentiality](#)
- [1.2 The Audit](#)
  - [1.2.1 Period Covered](#)
  - [1.2.2 Completeness and Accuracy of Information Provided by the Entity (IPE)](#)
  - [1.2.3 Audit Documentation](#)
    - [1.2.3.1 Observation](#)
    - [1.2.3.2 Inspection](#)
    - [1.2.3.3 Reperformance](#)
    - [1.2.3.4 Interview](#)
  - [1.2.4 Sampling](#)
  - [1.2.5 Data storage and Transmission](#)
  - [1.2.6 Certification Level](#)
- [1.3 Peer Review](#)
  - [1.3.1 Peer Review Process](#)
  - [1.3.2. Recommended Timeframe for Peer Review Process](#)
  - [1.3.3 Fee structure for Peer Review Process](#)
  - [1.3.4 CCSSA-PR Expectations](#)
  - [1.3.5 Dispute Resolution](#)
- [1.4 Approval](#)

[2. Professional Ethics](#)
- [2.1 CCSSA](#)
- [2.2 CCSSA-PR](#)

https://cryptoconsortium.org

Version 1.3-2022-9-15

3. Code of Professional Responsibility

4. Audit Flow
    4.1 Audit Flow Image
    4.2 Audit Flow Text

This guide has been created to assist CCSSA's in the performance of audits. Any concerns or questions may be directed to info@cryptoconsortium.org.

1. Audit Process

1.1 Appointment

1.1.1 Agreement

All CryptoCurrency Security Standard (CCSS) audit agreements must be written between the CCSSA and the entity and include the scope of the audit. Agreements must not include the CCSS Steering Committee or CryptoCurrency Certification Consortium (C4) and are directly between the CCSSA, CryptoCurrency Security Standard Auditor Peer Reviewer (CCSSA-PR), and the entity. As such, Appendix 1 must be signed by the CCSSA, the CCSSA-PR, and the entity in order for the audit to be recognized by C4. Appendix 1 must be included with the Summary Report on Compliance (SRoC).

Additional details about selecting a CCSSA-PR can be found in section 1.3.1 Peer Review Process.

1.1.2 Fees

1.1.2.1 Audit Fees

Audit fees will be determined between the CCSSA and the entity. It is the responsibility of the CCSSA to ensure sufficient time to complete the audit is reflected in the agreed upon fees.

Audit fees must also include the CCSSA-PR's fee and Listing Fee. The CCSSA-PR's fee will be forwarded to the CCSSA-PR by the CCSSA. C4 will send an invoice for the Listing Fee to the CCSSA after approving the SRoC.

1.1.2.2 Listing Fee

The listing fee is based on 2 types of entities: Merchants and Service Providers.

Merchants are defined as those who accept cryptocurrency payments for goods and services that customers do not use to conduct transactions. Merchants pay a flat listing fee of $1,000.

Service Providers are defined as those that provide goods and services that customers use to conduct cryptocurrency transactions. Service providers are separated into 2 types of pay structures: those who DO NOT charge a fee from customer/user transactions, and those who DO charge a fee from customer/user transactions.

Table 1.

	Merchants (Self Custody)	**Service Providers who DO NOT charge a fee from transactions**	**Service Providers who DO charge a fee from transactions**
Examples	Systems that manage only their own funds	Systems that have non-majority key custodians	Systems that custody assets as a service such as Exchanges and Custodians.
Cost of Listing Fee	$1,000 (flat rate)	$5,000 (flat rate)	$15,000 (flat rate)

1.1.3 Confidentiality

The CCSSA is responsible for ensuring that all agreements include a confidentiality clause in compliance with requirements of the jurisdiction the audit is being performed in.

1.2 The Audit

1.2.1 Period Covered

All CCSS audits cover a period of time prior to audit completion and will test the operating effectiveness of the control over this period of time. Audits are designed to be performed at least annually and cover the preceding 12 month period.

When a first time audit is performed the period covered may be 6 to 18 months prior to the audit, as determined by the CCSSA. It is recommended that first time audits are preceded by an Audit Readiness Assessment.

1.2.2 Completeness and Accuracy of Information Provided by the Entity (IPE)

The CCSSA is responsible for obtaining sufficient evidence pertaining to the completeness and accuracy of all information obtained in the performance of the CCSS audit.

This evidence and the procedures performed should also be documented in the Audit Documentation for a CCSSA-PR to be able to inspect and verify the accuracy and completeness of information.

The CCSSA is expected to inform the entity that significant changes to security practices and procedures between the audit and Summary Report on Compliance submission could invalidate the audit and must be disclosed to the CCSSA.

1.2.3 Audit Documentation

Audit Documentation consists of the records maintained by the CCSSA performing the audit to support the basis for the CCSSA's conclusions over the effectiveness of controls and CCSS Level obtained.

The audit documentation should, at a minimum, detail the following.

- Procedures performed to reach conclusion (ie. inspection, inquiry, reperformance, observation, etc.);
- Evidence of procedures performed over Information Produced by the Entity (IPE) to demonstrate completeness and accuracy;
- Rationale and methodology used when applying sampling over a population of items;
- Rationale for conclusion reached on the CCSS level of compliance;

The CCSSA must securely retain audit documentation for 7 years or as long as required by law in the jurisdiction they are operating in.

The following are examples of information/evidence that should be retained for IPE purposes:

1.2.3.1 Observation

If the CCSSA is observing a process, then they should record the following:

1. What process is being observed
2. Reference the policy, standards, and procedure documentation that the process is defined upon
3. Date and time and location of the observation
4. Who was undertaking the process - include full name and role of the person
5. The outcome of the process and any other pertinent events that are used as considerations by the CCSSA as to the compliance status
6. Any outstanding evidence that needs to be supplied and new actions that were identified out of the observation

1.2.3.2 Inspection

If the CCSSA is reviewing documentation such as policy, standards, procedures then record the following:

1. File name of the document
2. Title of the document
3. Purpose of the document
4. Version of the document
5. Owner of the document
6. When the document was last reviewed and updated
7. Location of the document - if viewing online documentation
8. CCSSA findings from the review of the document. This might be used for reporting on remediation such as the report is missing "x" which is required for CCSS compliance
9. Any outstanding evidence that needs to be supplied and new actions that were identified out of the inspection

If the CCSSA is reviewing records such as reports then record the following:

1. Name of record
2. Date and time of the records generation
3. Brief description of how the record is generated including what roles can generate the record
4. Purpose of the record
5. CCSSA findings from the review of the record
6. Any outstanding evidence that needs to be supplied and new actions that were identified out of the review

If the CCSSA is inspecting configuration data and data at rest, then record the following:

1. What is the device or system that the configuration data pertains to or where is the data located - e.g. in what database server, in what database, in what table?
2. Date and time of the configuration review and the name and title of person who provided access to the data
3. CCSSA findings from the review of the data
4. Any outstanding evidence that needs to be supplied and new actions that were identified out of the inspection

1.2.3.3 Reperformance

Note that reperformance as an evidence gathering technique will not frequently be utilized. Reperformance can be substituted by observation, inspection, and interviews

There may be an action that can be performed by the CCSSA where the risk of impacting the availability, confidentiality or integrity of the system and/or information is negligible. In that instance record the following:

1. What process is being undertaken by the CCSSA
2. Who authorized (in writing) that the CCSSA could undertake the process

3. Brief description of the process
4. The outputs of the process
5. CCSSA findings from the undertaking of the process
6. Any outstanding evidence that needs to be supplied and new actions that were identified out of the reperformance

1.2.3.4 Interview

For each interview conducted record the following:

1. Name of interviewee - full name and role
2. Date and time and location of the interview
3. Duration of the interview
4. Topics covered within the interview
5. Any outstanding evidence that needs to be supplied and new actions that were identified out of the interview

Ensure that notes are taken during the interview or if possible and with prior authorisation voice or video record the interview

CCSSA's should also consider the nature of the report generated. For standard and canned system reports, little additional testing would be required. For custom reports of ad-hoc queries, the CCSSA should consider additional procedures such as inspecting the query parameters or database query to ensure data produced is accurate and complete.

These considerations should take into account input, processing, and output risks around the report.

Example:

Where a CCSSA is testing controls such as new users added to the system, the CCSSA should obtain a list of all new users appointed or transfers between departments during the period directly from the entity's HR system. The CCSSA may inspect the parameters used while pulling this listing to ensure no data was excluded and the period covered is correct. Screenshots of the query and resulting output can be used as evidence of IPE procedures.

Where an entity has privacy concerns over this data, the CCSSA may observe them pulling the listing via a video call, noting the number of records and spots checks on the data. The entity can then anonymize data, leaving unique identifiers to be able to identify items, before sending the listing to the CCSSA.

The CCSSA can then use this listing and unique identifiers to select the sample for testing the control.

1.2.4 Sampling

Where a CCSSA is testing the operating effectiveness of a control over a period of time, a sampling approach should be followed. For a control with a high frequency of occurrence it is not practical to test all occurrences.

Audit sampling enables the CCSSA to obtain and evaluate audit evidence about some characteristic of the items selected in order to form or assist in forming a conclusion concerning the population from which the sample is drawn.

Sample size

The sample size can be determined by the application of a statistically based formula or through the exercise of professional judgment.

The CCSSA must document their rationale behind the sample size selected and consider the following factors:

- What a tolerable rate of deviation will be given the size of the population;
- What the likelihood and impact is of errors occurring given the procedure being tested;
- How critical the procedure is and the level of certainty required given its importance.

Example:

An example of a testing approach would be the following (this is only a guide and should not be used as your testing methodology)

Population Size	Low risk of failure / Low Importance	High risk of failure / High Importance
1(Annual)	1	1
4(Quarterly)	2	3
12(Monthly)	3	6
1-25(Occurrences)	5	10
26-50(Occurrences)	10	20
51-100(Occurrences)	20	30
101-X(Occurrences)	30	CCSSA judgment used

Items selected for testing

When identifying the items to be tested, the CCSSA can use professional judgment, random selection, or a combination of the two techniques.

When identifying items to test using professional judgment the CCSSA should consider factors such as the following:

- Items that are likely to be subject to manipulation;
- When the items occurred;
- Who performed the procedure;
- Items that are outliers in the general population, etc.

When identifying items using random selection the CCSSA should make use of a randomized sampling technique such as the following:

- Simple random sampling (i.e. using a random number generator within the range of the population);
- Systematic random sampling (Identifying a starting point and then selecting items at a specific interval from this point).

1.2.5 Data storage and Transmission

The CCSSA is responsible for ensuring all data related to the audit is transmitted and stored in a secure manner for the duration of the CoC and as legally required in the jurisdiction of the audit. In the event that an entity will not allow evidence storage outside of the entity's environment, the CCSSA should record the meta-data of the documentation reviewed such as file name, location of file within assessed entities environment, version number of documentation, summary of document content, etc. In this case, the entity must give access to this documentation to the CCSSA-PR.

The CCSSA is also responsible for ensuring all data protection requirements (General Data Protection Regulation (GDPR) or equivalent) are met for the jurisdiction the audit is being performed in.

1.2.6 Certification Level

Entities will be certified at the lowest level of any Aspect, regardless of other Aspect's Compliance Status. In the example below, CCSS Level 1 would be granted.

CCSS Aspect Compliance Status

Aspect	CCSS Level 1	CCSS Level 2	CCSS Level 3
Key/Seed Generation		✔	
Wallet Creation		✔	
Key Storage			✔
Key Usage		✔	
Key Compromise Policy	✔		
Keyholder Grant/Revoke Policies & Procedures		✔	
Security Tests/Audits		✔	
Data Sanitization Policy			✔
Proof of Reserve		✔	
Audit Logs		✔	

1.3 Peer Review

All CCSS audits will be subject to a peer review process after the CCSSA has completed their evidence gathering and documentation. CCSSA's must follow the CCSSA-PR selection process as explained below. CCSSAs will securely submit their Audit Documentation as well as conclusion on the CCSS Level certification obtained to a CCSSA-PR.

The CCSSA-PR must be copied on final submission of the audit to C4 in order for the certification to be issued.

1.3.1 Peer Review Process

Prior to signing the audit agreement with the entity, the CCSSA must complete the Intent to Audit form found here: https://cryptoconsortium.org/intent-to-audit/. C4 will then email the CCSSA a list of randomly selected CCSSA's. The CCSSA must select from the Peer Reviewer Options List (PROL) to perform the peer review and contact them. The CCSSA-PR's fee will be included in the CCSSA's audit agreement with the entity.

In the case of sufficient evidence a CCSSA-PR has a material conflict of interest or another reason to not perform the review, the CCSSA must contact another CCSSA-PR on the PROL.

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 these queries.

1.3.2. Recommended Timeframe for Peer Review Process

Procedure	Recommended Timeframe
Peer review	10 working days
Resolution of queries	10 working days

1.3.3 Fee structure for Peer Review Process

The CCSSA is responsible for negotiating directly with the CCSSA-PR. While C4 cannot recommend any specific fees, we do recommend considering the scope of the audit when choosing the Peer Review Fee.

1.3.4 CCSSA-PR Expectations

All CCSSA's will be required to make themselves available to perform one Peer Review for every audit they complete.

1.3.5 Dispute Resolution

Any dispute arising out of the peer review process shall be arbitrated by the CCSS Steering Committee. The committee's decision will be final and binding. Audit Documentation for the disputed aspect will be securely submitted to the committee at CCSS_Submissions@cryptoconsortium.org. This means using encrypted, password protected, Zipped files or something comparable. The committee shall review the evidence and provide a decision within 15 business days.

1.4 Approval

After CCSSA-PR completes Peer Review, CCSSA must send the following to CCSS_Submissions@cryptoconsotritum.org & copy the CCSSA-PR:

1. Summary Report on Compliance (SRoC)
2. Appendix I
3. Entity's CoC Listing Information (entity website, entity contact, system audited, entity logo at least 500x500 pixels in size)
4. Listing Fee total cost

C4 will then send an invoice for the Listing Fee to the CCSSA.Once paid, C4 will provide CCSSA with CoC and Badge for CCSSA to provide to the entity.

Certificates of Completion can be viewed and verified at the following link: https://cryptoconsortium.org/completed-ccss-audits/

2. Professional Ethics

2.1 CCSSA

CCSSAs must avoid any potential conflict of interest. This may include current or previous employment, familial relationships, financial interest (such as tokens or equity held), or any other matters that may constitute a conflict of interest.

Failure to recuse oneself due to any conflicts of interest will result in disciplinary action, up to and including loss of CCSSA certification.

2.2 CCSSA-PR

CCSSA-PR must avoid any potential conflict of interest. This may include current or previous employment, familial relationships, financial interest (such as tokens or equity held), or any other matters that may constitute a conflict of interest.

Failure to recuse oneself due to any conflicts of interest will result in disciplinary action up to and including loss of CCSSA certification.

3. Code of Professional Responsibility

This Code of Professional Responsibility defines the expectations for professional and ethical conduct of all CCSSAs. All CCSSAs must advocate, adhere to, and support the following principles:

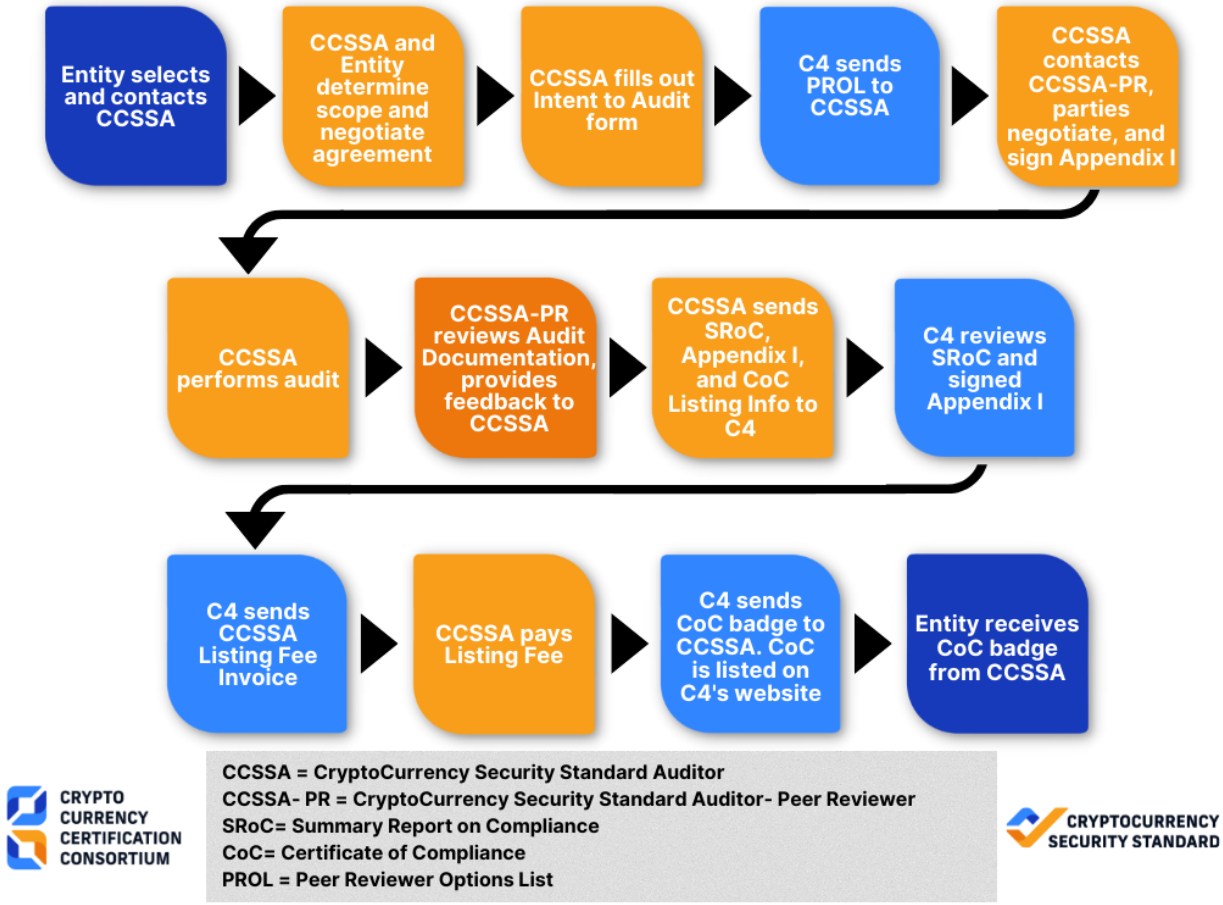
1. Actions must reflect professional competence and due care, and be in accordance with standards and guidance.
    a. Perform each aspect of your work honorably, responsibly, diligently and objectively.
    b. Act in the best interest of the entities to which you provide services or support, and keep them apprised of changes to CryptoCurrency Certification Consortium (C4) standards and guidance.
    c. Render only those services for which you are fully competent and qualified to perform.
    d. Promote current information security best practices and standards.
2. Perform duties in a way that supports data security, confidentiality and integrity.

    a. Respect and safeguard confidential, proprietary, or otherwise sensitive information with which you come into contact during the course of professional activities.
    b. Immediately notify appropriate authorities and/or industry personnel as required should you discover or suspect a compromise or breach.
3. Operate with integrity.
    a. Refrain from conduct that could damage or reflect poorly on the reputation of C4, its standards, your profession, or the practice of colleagues, clients or employers.
    b. Refrain from any activities that might constitute a conflict of interest. A conflict of interest arises when an individual finds themselves occupying two social roles simultaneously which generate opposing benefits or loyalties.
    c. Maintain honesty and accuracy when delivering any information or guidance related to C4 programs, standards and related documentation.
    d. Report ethical violations to C4 in a timely manner.
4. Comply with all applicable laws, regulations and industry standards.

CCSSAs who violate any of the foregoing principles will be subject to disciplinary action by C4, including but not limited to revocation of certification.

4. Audit Flow

4.1 Audit Flow Image



4.2 Audit Flow Text

1. Entity selects and contacts CCSSA
2. CCSSA and Entity determine scope and negotiate agreement
3. CCSSA fills out Intent to Audit form
4. C4 sends PROL to CCSSA
5. CCSSA contacts CCSSA-PR, parties negotiate, and sign Appendix 1
6. CCSSA performs audit
7. CCSSA-PR reviews Audit Documentation, provides feedback to CCSSA
8. CCSSA sends SRoC, Appendix 1, and listing info to C4

9. C4 reviews SRoC and signed Appendix 1
10. C4 sends CCSSa Listing Fee Invoice
11. CCSSA pays Listing Fee
12. C4 sends CoC and badge to CCSSA. CoC is listed on C4's website
13. Entity receives CoC badge from CCSSA

Acronym List:

CCSSA= CryptoCurrency Security Standard Auditor
CCSSA-PR= CryptoCurrency Security Standard Auditor - Peer Reviewer
SRoC= Summary Report on Compliance
CoC= Certificate of Compliance
PROL= Peer Reviewer Options List