CryptoCurrency Security Standard Auditor (CCSSA) Guide

https://cryptoconsortium.org

Version 2.1-2026-8-4

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 audited 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 C4's 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, paid by the audited system's entity to the CCSSA, is based on table 1.

When multiple systems (up to 3) are covered in the same audit, C4 only charges the listing fee of the most expensive system. When auditing 4-6 systems, C4 only charges the listing fee of the two most expensive systems, and so on.

Systems that maintain a Certificate of Compliance without letting it lapse receive a 25% discount on the listing fee.

Table 1.

Table 1 — CRYPTOCURRENCY SECURITY STANDARD

	Self Custody	Qualified Service Provider	Full System
Definition	Systems that hold all keys to the system that controls the entity's own funds.	A CCSS Qualified Service Provider (QSP) is a system that meets many of the requirements for CCSS certification with the exception of the few requirements that another system has control over. A QSP is a system that facilitates a subset of custody services to other systems and therefore is only required to meet certain requirements. This means that if a system uses a QSP, the audit focus is only on the few remaining requirements to become certified.	An information system that meets all applicable CCSS requirements in totality. In situations where an information system utilizes a CCSS certified Qualified Service Provider (QSP) information system (e.g. a wallet infrastructure provider's wallet software) as part of their information system, some CCSS requirements may be met by the QSP information system, as determined by the CCSSA conducting the CCSS audit.
Examples	A Web3 marketing firm that accepts cryptocurrency and controls the private keys for the system used to control their funds.	A system such as a Hardware Security Module (HSM) or Multi-Party Computation (MPC) that provides key management services that are used by another entity's system.	A system that can reach quorum without any additional system. A system such as an exchange that incorporates a QSP into their system.
Listing Fee* (annual)	$250	$2,000	$3,500

* When multiple systems (up to 3) are covered in the same audit, C4 only charges the listing fee of the most expensive system. When auditing 4-6 systems, C4 only charges the listing fee of the two most expensive systems, and so on.
* Systems that maintain Certificate of Compliance receive a 25% discount on annual listing fee.

If you have any questions, please reach out to info@cryptoconsortium.org
CCSS™ Version 8.1 | https://cryptoconsortium.org

1.1.3 Confidentiality

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

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 requirement 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 Redacted Report on Compliance for the CCSSA-PR to inspect and verify the accuracy and completeness of the 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 requirements and CCSS Level obtained.

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

- Procedures performed to reach conclusion (i.e. review, inspection, observation, interview, reperformance.);

- 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;

A comparable control is a control put in place by the entity that provides equivalent or comparable protection to the control defined in the CCSS. The CCSSA can use their professional judgment where organizational controls do not meet CCSS controls descriptions but provide a similar level of protection.

A requirement can be marked as Not Applicable if a requirement does not apply to the assessed entity's environment. CCSSA's must provide evidence that testing was undertaken to confirm that the assessed entity's environment does not support or provide a facility that would meet the requirement's intent when marking a control as Not Applicable.

Example 1
1.01.2.2 In cases where key material is generated without the use of software, the generation methodology is validated to ensure determinism is not present.

If the information system being audited uses software to generate the entropy when creating keys or seeds then this requirement is Not Applicable

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/or 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

1.2.3.3 Review

If the CCSSA is reviewing documentation 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

1.2.3.3 Inspection

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

1.2.3.4 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 authorization, 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.

1.2.3.5 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

1.2.4 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 Certificate of Compliance 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.

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 Reconciliation of Standard Versions

If a QSP's CCSS certification is for a previous version of CCSS, when a new version of CCSS is released, the entity using the QSP within its CCSS Trusted Environment can accept the QSP's CCSS certification until the end of the assigned grace period (see Transition Guidelines Document). Once the assigned grace period has been reached, the QSP must audit and certify under the new CCSS version.

For example, if a QSP is certified under CCSS version 8.1 and a Full System, using that QSP within the CCSS Trusted Environment is auditing and certifying under CCSS version 9.0, then the QSP's CCSS version 8.1 certification is acceptable until the end of the grace period allocated to the QSP.

1.2.7 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 Generation Material		X	
Wallet Generation		X	
Key Material Storage			X
Key Material Access		X	
Key Material Usage		X	
Data Sanitization Documentation			X
Security Tests/Audits	X		
Log and Monitor		X	
Governance and Risk		X	
Key Compromise Documentation	X		

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 (including reports of what types of evidence were provided by entity) 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 CCSSAs. This list is randomized to prevent conflicts of interest & collusion. The CCSSA must select from the Peer Reviewer Options List (PROL) to perform the Peer Review. Contacting a CCSSA-PR, negotiating payment, and verifying that the Peer Reviewer's certification will be valid for the duration of the audit is the CCSSAs responsibility.

Before the CCSSA-PR accepts the engagement, the CCSSA should provide sufficient information (such as the entity name and system name or scope) to allow the prospective CCSSA-PR to determine whether they are able to perform the peer review.

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.

In the case of sufficient evidence that attempts to engage all potential CCSSA-PRs from a PROL have been unsuccessful, an additional PROL may be requested. Once an additional PROL is sent, all prior PROLs are no longer valid. The Peer Reviewer must be selected from the most recent PROL.

In the rare event where, after accepting the engagement and signing Appendix 1, a CCSSA-PR determines that they are unable to perform the peer review, the CCSSA should notify C4 of the circumstances of changing the CCSSA-PR.

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.

The Peer Review of the first audit conducted by a CCSSA is required to be completed by a current member of the CCSS Steering Committee. This ensures that the audit is conducted with the requisite rigor to uphold the standard. The CCSSA must still complete the Intent to Audit form and will receive contact information for the CCSS Steering Committee Member from C4.

A CCSSA cannot conduct a peer review for the same entity for three years after their initial peer review of that entity. However, a different CCSSA from the same organization as the original CCSSA-PR can perform a peer review for the same entity, if they are on the PROL.

If a CCSSA has conducted an audit of a system, they are not eligible to perform the peer review for the next three audits of that system. Adherence to these rules is the responsibility of the CCSSA conducting the audit.

1.3.1.1 Communication Plan

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

1.3.1.2 Report on Compliance Redaction Process

Before submitting audit documentation to the CCSSA-PR the CCSSA will make a copy of the Report on Compliance (RoC) audit report and from that copy, redact all sensitive information and personal identifiable information (PII) of the audited entity's environment, information

systems being audited, and personnel interviewed as part of the audit process. The output of this process will be the Redacted RoC. The primary responsibility of the CCSSA-PR is to review the redacted RoC and ascertain that the CCSSA conducted thorough evidence-gathering techniques.

Note that the CCSSA-PR will not have a confidentiality agreement or other permissions with the entity under audit. Therefore the CCSSA-PR cannot view the audit evidence collected by the CCSSA and the RoC is redacted for the peer review process. Additionally, CCSSA-PRs must communicate only with the CCSSA whose audit they are reviewing, and have no contact with the entity being audited. See 1.3.5 for information on dispute resolution.

1.3.1.3 Submission of Redacted RoC to CCSSA-PR

Once the CCSSA has created the Redacted RoC it is recommended that the CCSSA submits the Redacted RoC to the entity under audit to seek approval to release the Redacted RoC to the CCSSA-PR. This is to ensure that no sensitive information or PII remains within the redacted RoC.

The CCSSA will not share or make available any of the evidence collected during the audit to the CCSSA-PR.

1.3.1.4 Access Control Plan

During the kickoff meeting, an Access Control Plan should also be established. 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. Appropriate access controls must be implemented for the redacted RoC before the CCSSA-PR has access to the redacted RoC. The access controls that will be implemented must be agreed upon by both the CCSSA and CCSSA-PR in writing. 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 text.

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

1.3.1.5 Peer Review Estimate on Effort

Based on previous CCSS Redacted RoC peer reviews, the estimated effort to conduct a Peer Review is approximately 10-15 hours, and varies depending on the system or systems being audited.

Note that the CCSSA-PR should consider an additional allowance of 1-2 hours to take into account additional reviews of the changed sections of the Redacted RoC if the CCSSA-PR requires changes. The CCSSA-PR reviews statements made in the Redacted RoC, an example of which is on the resources page available only to CCSSAs.

If more in depth remediation is required, then the CCSSA and CCSSA-PR will need to enter into negotiations for additional billable hours.

1.3.1.6 Peer Review Focus and Goal

The peer review process does NOT include the review of audit evidence collected by the CCSSA during the audit. The CCSSA-PR is instead required to review the evidence gathering techniques (interviews, inspection, observation, review) undertaken by the CCSSA during the audit and documented in the Redacted RoC. The goal is to ensure that the CCSSA collected a broad range of evidence in order to have the ability to form a correct opinion on whether applicable CCSS requirements were met.

For example, it would be expected that a general auditing process would be undertaken for the bulk of the applicable CCSS requirements. This would be done by first reviewing policy/standards/procedures to understand the entity's goals and intent for the information system. Secondly, reviewing interviews of personnel who use the policy/standards/procedures in order to complete their assigned tasks. And thirdly, inspecting outputs of the processes undertaken such as configurations of devices, Business As Usual (BAU) reports, and change requests to ensure that the policy/standards/procedures are being followed.

This structured approach maintains the highest standards of professionalism and confidentiality within the auditing framework.

1.3.1.7 Peer Review Feedback to CCSSA

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.

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.

1.3.1.8 Completion of Peer Review Process

CCSSA-PR must provide written confirmation to the CCSSA that the peer review process is complete. If any changes are made during the peer review process, the CCSSA must update the RoC with those changes, and the CCSSA-PR must then re-review the Redacted RoC and approve. After this, the SRoC is created by the CCSSA and must be signed by both the CCSSA and the CCSSA-PR.

The Redacted RoC must be retained as part of the stored audit documentation for the required retention period.

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@cryptoconsortium.org & copy the CCSSA-PR:

1. Summary Report on Compliance (SRoC) in PDF format
2. Appendix I
3. Entity's CoC Listing Information (entity website, entity contact, system audited, entity logo of file type .jpg or .png 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 Compliance 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

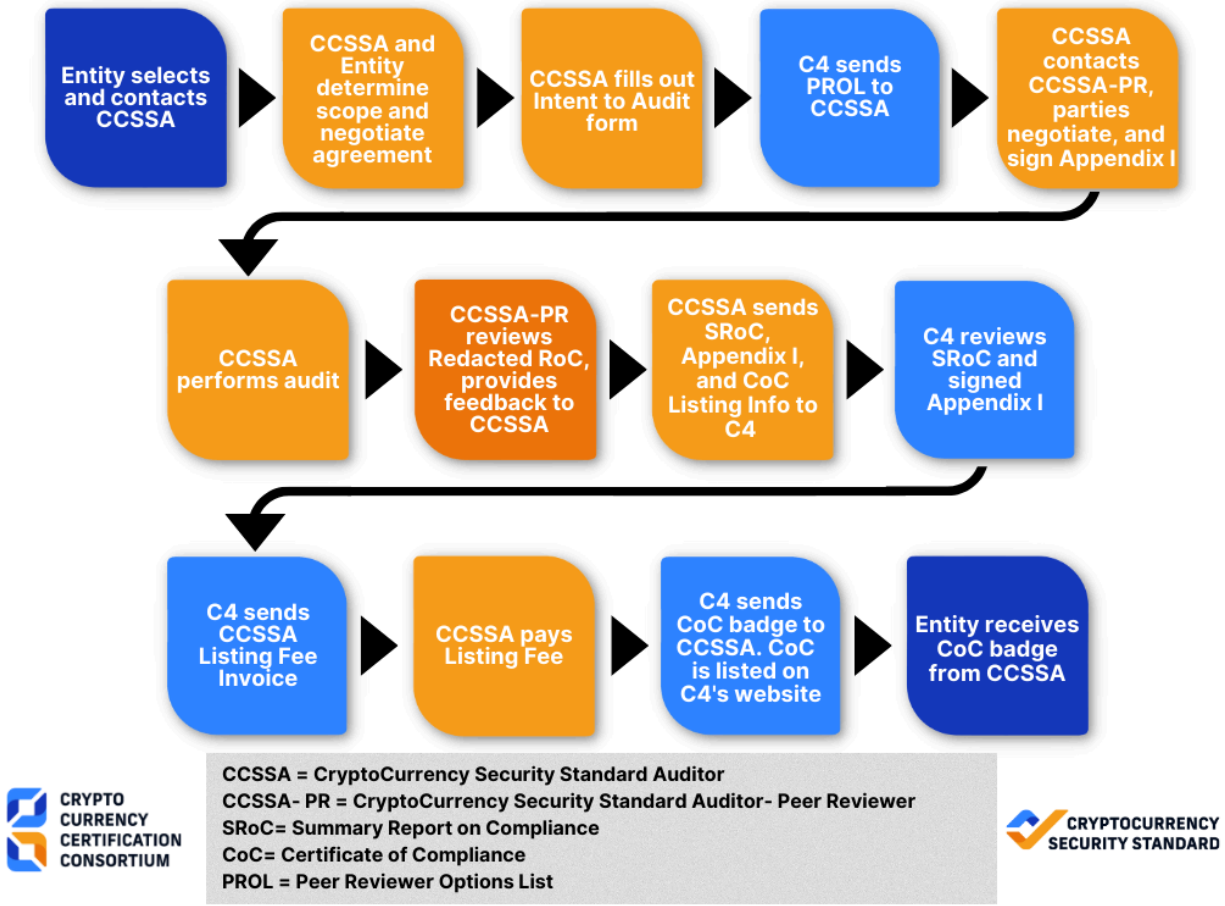
This Code of Professional Responsibility defines the expectations for professional and ethical conduct of all CCSSAs. All CCSSAs must advocate, adhere to, and support the following principles:

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. Refrain from auditing a system upon which you've 1) conducted a readiness assessment where the outcome shows the system is not audit-ready and 2) assisted in the development of the system intended for audit. A different CCSSA should either perform the system development or the audit to maintain ethical standards.
    d. Maintain honesty and accuracy when delivering any information or guidance related to C4 programs, standards and related documentation.
    e. 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 Redacted RoC, 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