Cryptocurrency Security Standard

Report on Compliance (RoC)

CCSS Version 8.1 – May 2023

Table of Contents

[Document Template History 2](#_heading=h.3rdcrjn)

[Document Version History 2](#_heading=h.32hioqz)

[About the CryptoCurrency Security Standard (CCSS) 2](#_heading=h.1hmsyys)

[Relationship to Other Standards 3](#_heading=h.41mghml)

[CCSS Audit Process 3](#_heading=h.2grqrue)

[CCSS Disputes 4](#_heading=h.vx1227)

[Audit Finding Statuses 4](#_heading=h.3fwokq0)

[Contact Information 5](#_heading=h.1v1yuxt)

[Audited Organization 5](#_heading=h.4f1mdlm)

[CCSS Auditor (CCSSA) 5](#_heading=h.2u6wntf)

[CCSS Peer Reviewer (CCSS-PR) 6](#_heading=h.19c6y18)

[Summary of Audit 6](#_heading=h.3tbugp1)

[CCSS Trusted Environment Summary 7](#_heading=h.28h4qwu)

[Trusted Environment 7](#_heading=h.nmf14n)

[Validation of Trusted Environment 8](#_heading=h.37m2jsg)

[Evidence Retention 8](#_heading=h.1mrcu09)

[Detailed Findings 10](#_heading=h.46r0co2)

[Cryptographic Asset Management 10](#_heading=h.2lwamvv)

[Aspect 1.01: Key/Seed Generation 10](#_heading=h.111kx3o)

[**Aspect Control 1.01.1: Operator-Created Key / Seed 11**](#_heading=h.3l18frh)

[**Aspect Control 1.01.2: Creation methodology is validated 15**](#_heading=h.206ipza)

[**Aspect Control 1.01.3: DRBG Compliance 17**](#_heading=h.4k668n3)

[**Aspect Control 1.01.4: Entropy Pool 19**](#_heading=h.2zbgiuw)

[Aspect 1.02: Wallet Creation 20](#_heading=h.1egqt2p)

[**Aspect Control 1.02.1: Multiple keys for signing 20**](#_heading=h.3ygebqi)

[**Aspect Control 1.02.2: Redundant key for recovery 21**](#_heading=h.2dlolyb)

[**Aspect Control 1.02.3: Geographic distribution of keys 22**](#_heading=h.sqyw64)

[**Aspect Control 1.02.4: Organizational distribution of keys 23**](#_heading=h.3cqmetx)

[**Aspect Control 1.02.5: Documented wallet creation policy 24**](#_heading=h.1rvwp1q)

[Aspect 1.03: Key Storage 1](#_heading=h.4bvk7pj)

[**Aspect Control 1.03.1: Primary keys are stored encrypted 1**](#_heading=h.2r0uhxc)

[**Aspect Control 1.03.2: Backup key exists 27**](#_heading=h.1664s55)

[**Aspect Control 1.03.3: Backup key has environmental protection 28**](#_heading=h.3q5sasy)

[**Aspect Control 1.03.4: Backup key is access-controlled 32**](#_heading=h.25b2l0r)

[**Aspect Control 1.03.5: Backup key has tamper-evident seal 33**](#_heading=h.kgcv8k)

[**Aspect Control 1.03.6: Backup key is encrypted 33**](#_heading=h.34g0dwd)

[Aspect 1.04: Key Usage 1](#_heading=h.1jlao46)

[**Aspect Control 1.04.1: Key access requires user/pass/nth factor 35**](#_heading=h.43ky6rz)

[**Aspect Control 1.04.2: Keys are only used in a trusted environment 37**](#_heading=h.2iq8gzs)

[**Aspect Control 1.04.3: Operator reference checks 38**](#_heading=h.xvir7l)

[**Aspect Control 1.04.4: Operator ID checks 39**](#_heading=h.3hv69ve)

[**Aspect Control 1.04.6: Spends are verified before signing 1**](#_heading=h.1x0gk37)

[**Aspect Control 1.04.7: No two keys are used on one device 1**](#_heading=h.4h042r0)

[**Aspect Control 1.04.8: DRBG Compliance 43**](#_heading=h.2w5ecyt)

[Aspect 1.05: Key Compromise Policy 45](#_heading=h.1baon6m)

[**Aspect Control 1.05.1: KCP Exists 46**](#_heading=h.3vac5uf)

[**Aspect Control 1.05.2: KCP Training and Rehearsals 49**](#_heading=h.2afmg28)

[Aspect 1.06: Keyholder Grant/Revoke Policies and Procedures 50](#_heading=h.pkwqa1)

[**Aspect Control 1.06.1: Grant/Revoke Procedures/Checklist 51**](#_heading=h.39kk8xu)

[**Aspect Control 1.06.2: Requests made via Approved Communication Channel 52**](#_heading=h.1opuj5n)

[**Aspect Control 1.06.3: Grant/Revoke Audit Trail 53**](#_heading=h.48pi1tg)

[Operations 54](#_heading=h.2nusc19)

[Aspect 2.01: Security Tests / Audits 54](#_heading=h.1302m92)

[**Aspect Control 2.01.1: Security Audit 55**](#_heading=h.3mzq4wv)

[Aspect 2.02: Data Sanitization Policy 58](#_heading=h.2250f4o)

[**Aspect Control 2.02.1: DSP Exists 58**](#_heading=h.haapch)

[**Aspect Control 2.02.2: Audit Trail of all media sanitization 60**](#_heading=h.319y80a)

[Aspect 2.03: Audit Logs 61](#_heading=h.2fk6b3p)

[**Aspect Control 2.03.1: Application Audit Logs 1**](#_heading=h.upglbi)

[**Aspect Control 2.03.2: Backup of Audit Logs 63**](#_heading=h.3ep43zb)

[Audit Evidence 64](#_heading=h.1tuee74)

[Interviews Conducted [INTERVIEW] 64](#_heading=h.4du1wux)

[Documentation Reviewed [DOCUMENT] 65](#_heading=h.2szc72q)

[Process Observations [OBSERVATION] 1](#_heading=h.184mhaj)

[Inspections [INSPECTION] 65](#_heading=h.3s49zyc)

[CCSS Committee Decisions [CCSS\_DECISION] 65](#_heading=h.279ka65)

# 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. |

# About the CryptoCurrency Security Standard (CCSS)

The CryptoCurrency Security Standard (CCSS) is a set of requirements for all information systems that make use of cryptocurrencies, including exchanges, web applications, and cryptocurrency storage solutions. By standardising the techniques and methodologies used by systems around the globe, end-users will be able to easily make educated decisions about which products and services to use and with which companies they wish to align.

## Relationship to Other Standards

CCSS is designed to complement existing information security standards (i.e. ISO 27001:2013) by introducing guidance for security best practices with respect to cryptocurrencies such as Bitcoin. CCSS is not designed to substitute or replace these standards; in fact, following the CCSS to the letter while ignoring standards like ISO 27001:2013 will likely lead to compromise. CCSS is a cryptocurrency standard that augments standard information security practices. As with any standard, knowledgeable and experienced security professionals and/or auditors are necessary when implementing any information system to ensure coverage of all classes of attack as well as the appropriate handling of all potential risks.

## CCSS Audit Process

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. All audits performed by CCSSAs are reviewed by a CCSSA-Peer Reviewer before C4 certifies an entity.

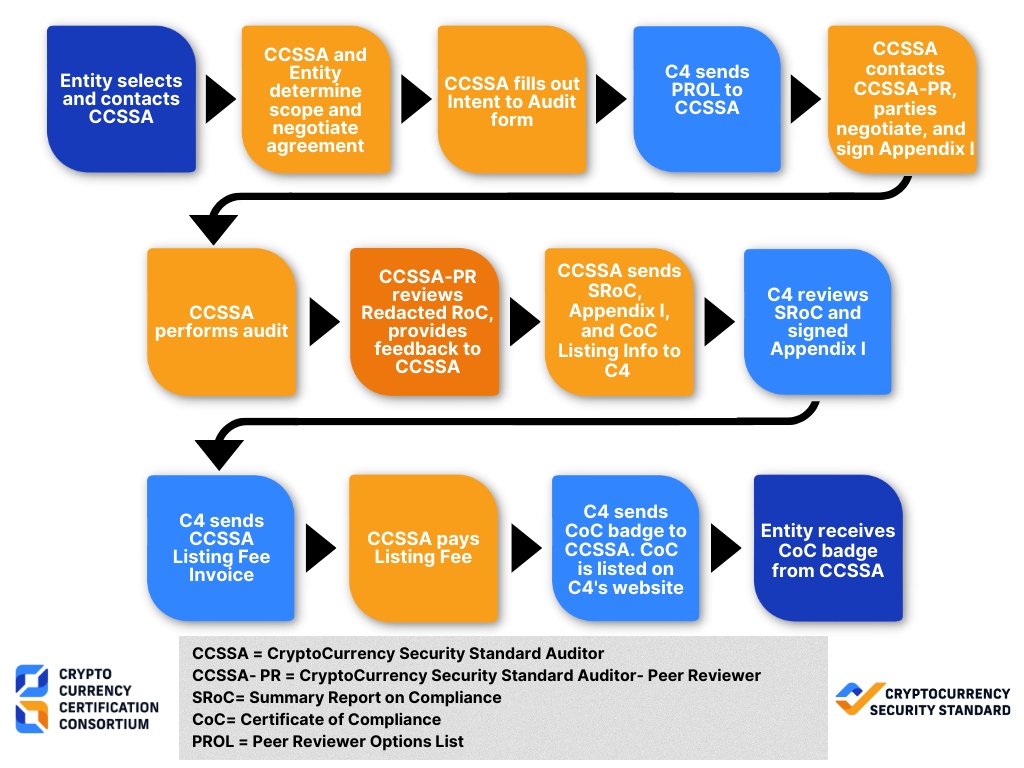


Figure 1: CCSS Audit Process

## CCSS Disputes

Any dispute arising out of the peer review process shall be arbitrated by the CCSS Steering Committee.

# Audit Finding Statuses

Each of the aspects from the CCSS has an audit finding status, these are described in the table below.

| **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 put in place 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 that are within a system’s control were shown to meet the requirement as written in the CCSS, however there are elements that lay beyond the audited system’s control. This qualifies the process to be found “in-place” when implemented by a consumer system that makes use of the audited system as a service provider. |
| *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* | Indicates that the requirement does not apply to the assessed entity’s requirement and 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. |

# Contact Information

## Audited Organization

| **Organization Name** |  |
| --- | --- |
| **Organization Website URL** |  |
| **Organization Mailing Address** |  |
| **Organization Contact Name** |  |
| **Organization Contact Phone** |  |
| **Organization Contact Email** |  |

## CCSS Auditor (CCSSA)

| **CCSSA Name** |  |
| --- | --- |
| **CCSSA Organization** |  |
| **CCSSA Organization Website** |  |
| **CCSSA Certificate Number** |  |
| **CCSSA Contact Phone** |  |
| **CCSSA Contact Email** |  |

## CCSSA Peer Reviewer (CCSSA-PR)

| **CCSSA-PR Name** |  |
| --- | --- |
| **CCSSA-PR Organization** |  |
| **CCSSA-PR Organization Website** |  |
| **CCSSA-PR Certificate Number** |  |
| **CCSSA-PR Contact Phone** |  |
| **CCSSA-PR Contact Email** |  |

# Summary of Audit

| **Audit Testing Period** | *Provide audit testing dates.* |
| --- | --- |
| **Demonstrated CCSS Level** | *Provide detail as to what CCSS designation (Self Custody, Qualified Service Provider or Full System) was met and the CCSS Level obtained.* |
| **CCSSA Explanation of Level Audit** | *Explain what roles, processes, and technology components where interviewed, inspected and reviewed to reach an opinion on CCSS Level obtained.* |

The below table summarises the demonstrated levels for each Aspect as demonstrated by the audited organization.

| **Aspect** | **Level 1** | **Level 2** | **Level 3** |
| --- | --- | --- | --- |
| 1.01 Key / Seed Generation | ☐ | ☐ | ☐ |
| 1.02 Wallet Creation | ☐ | ☐ | ☐ |
| 1.03 Key Storage | ☐ | ☐ | ☐ |
| 1.04 Key Usage | ☐ | ☐ | ☐ |
| 1.05 Key Compromise Policy | ☐ | ☐ | ☐ |
| 1.06 Keyholder Grant / Revoke Procedures / Checklist | ☐ | ☐ | ☐ |
| 2.01 Security Tests / Audits | ☐ | ☐ | ☐ |
| 2.02 Data Sanitization Policy | ☐ | ☐ | ☐ |
| 2.03 Audit Logs | ☐ | ☐ | ☐ |

# 

# CCSS Trusted Environment Summary

## Trusted Environment

| **Overview of CCSS Trusted Environment (in-scope people, process and technology components for this CCSS audit)** | *Define the CCSS Trusted Environment (in-scope environment for audit) people, processes and technology components.* |
| --- | --- |
| *For each component of the CCSS Trusted Environment, specify and provide a description (add or remove lines as required)..* | |
| **Component Name** | **Component Description** |
|  |  |
|  |  |
|  |  |

## Validation of Trusted Environment

| **Describe How the Trusted Environment was validated** | *Provide information on how the CCSS Trusted Environment was defined. E.g. What processes were reviewed? What policy, standards and procedures were reviewed? What personnel roles were interviewed? What systems were inspected?* |
| --- | --- |
| **Provide the name of the CCSSA who confirms that the validated environment has been accurately identified and included in the scope of audit.** |  |

# Evidence Retention

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. C4 will not view documentation of evidence outside the Summary Report on Compliance. The CCSS steering committee shall review evidentiary documentation in the case of a peer review dispute.

| **Indicate whether the evidence is held by the CCSSA or the audited organization.** |  |
| --- | --- |
| *If held by the CCSSA:* | |
| **Provide the name of the CCSSA who confirms that the evidence has been stored in a location where it can be retrieved for the required period.** |  |
| *If held by an organization other than the CCSSA (such as the audited organization):* | |
| **Provide the name of the organization responsible for evidence retention.** |  |
| **Provide the name of the assessor who confirms that the organization has been informed of the retention requirements.** |  |
| **Provide the name of the member of the organization to attest that the evidence retention requirements will be met.** |  |

# Detailed Findings

## Cryptographic Asset Management

### Aspect 1.01: Key/Seed Generation

*This aspect covers the generation of cryptographic keys and seeds that will be used within a digital asset and blockchain protocol. The secure creation of cryptographic keys and seeds requires two things to be secure: confidentiality and unpredictable numbers. Confidentiality is required to ensure that the newly created keys or seeds are not read/copied by an unintended party. Nondeterministic and unpredictable numbers are required to ensure the newly created key cannot be guessed or determined by an unintended party. Each of the goals listed provide assurance that the keys and/or seeds are created in a confidential and un-guessable manner.*

#### **Aspect Control 1.01.1: Operator-Created Key / Seed**

| ***LEVEL I REQUIREMENTS*** | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Requirement** | 1.01.1.1 The cryptographic keys and seeds are created by the actor who will be using it. | | | | | | | |
| **Audit Finding Summary** | **In-Place** | **In-Place with Comparable Control** | | **Qualified for In-Place** | | **Not In-Place** | | **Not Applicable** |
| ☒ | ☐ | | ☐ | | ☐ | | ☐ |
| **CCSSA Findings** | [ENTITY] key generation mechanisms are executed during account setup by code executed within the SGX (“Intel Software Guard Extensions”) secure enclave as part of the customer’s account setup. The MPC key is comprised of three MPC key shares. Two of the key shares are stored within the [ENTITY] environment and are used by automated signing agents. The third key share is installed on the customers device (usually a mobile device) within the Trusted Execution Environment of that device (TEE) and used by the [ENTITY] automated signing agent installed on the customers same device. | | | | | | | |
| **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** |  | | | | | | |
| **Requirement** | 1.01.1.2 In cases where an automated agent will make use of a cryptographic key/seed, it is required that the administrator of that system generate the key/seed on a suitable offline system with sufficient entropy, have this key/seed transferred securely onto the target device, and then securely deleted using CCSS-compliant data sanitization techniques to protect the confidentiality of the key/seed. | | | | | | | |
| **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** |  | | | | | | |
| **Inspections** |  | | | | | | |
| **CCSS Committee Decisions** |  | | | | | | |
| **Documents** |  | | | | | | |
|  | | | | | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | | | | |
| **Requirement** | 1.01.1.3 A digital signature for the key creation software is generated, published, and validated prior to each execution. | | | | | | | |
| **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** |  | | | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | | | | |
| No Level III Requirements. | | | | | | | | |

#### **Aspect Control 1.01.2: Creation methodology is validated**

| ***LEVEL I REQUIREMENTS*** | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| No Level I Requirements | | | | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | | | |
| **Requirement** | 1.01.2.1 The key or seed generation methodology is validated prior to use. Software does not include features that restrict which values can be used. Software does not include features that store or transmit data to another actor, unless that feature enhances security (e.g. DRBGs) | | | | | | |
| **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** | |  | | | | |
| **Requirement** | 1.01.2.2 In cases where keys or seeds are created without the use of software (e.g., dice, a deck of cards, or other non-digital source of entropy), the creation methodology must be validated to ensure determinism is not present (e.g., there are no weighted dice, each card in the deck is unique). | | | | | | |
| **Audit Finding Summary** | **In-Place** | **In-Place with Comparable Control** | | **Qualified for In-Place** | | **Not In-Place** | **Not Applicable** |
| ☐ | ☐ | | ☐ | | ☐ | ☐ |
| **CCSSA Findings** | [ENTITY] key creation processes are implemented by code only. There are no key generation processes within the in-scope environment that implements non-software key creation processes. | | | | | | |
| **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** | |  | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | | | |
| No Level III Requirements | | | | | | | |

#### **Aspect Control 1.01.3: DRBG Compliance**

| ***LEVEL I REQUIREMENTS*** | | | | | |
| --- | --- | --- | --- | --- | --- |
| No Level I Requirements | | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | |
| No Level II Requirements | | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | |
| **Requirement** | 1.01.3.1 The key or seed is generated using either a 1) Deterministic Random Bit Generator (DRBG) that conforms to NIST SP 800-90A, and has been seeded with at least two separate cryptographically secure sources of entropy that have been combined in a cryptographically secure manner (e.g., SHA256[UnguessableFactor1 + UnguessableFactor2]) or 2) a Non-deterministic Random Bit Generator (NRBG), or a “True Random Number Generator” (TRNG) that passes industry-standard statistical tests for randomness such as DIEHARD, Crypt-X, or NIST STS. The Dual\_EC DRBG has been demonstrated to be vulnerable and thus must not be used. | | | | |
| **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** |  | | | |
| **Requirement** | 1.01.3.2 The key/seed generation process has been documented including a detailed run book showing all steps performed and signed-off by different parties that each procedure was performed and checked. The documentation shows clear segregation of duties and/or the presence of an independent third party to observe and validate the procedures. | | | | |
| **Audit Finding Summary** | **In-Place** | **In-Place with Comparable Control** | **Qualified for In-Place** | **Not In-Place** | **Not Applicable** |
| ☐ | ☐ | ☐ | ☐ | ☐ |
| **CCSSA Findings** |  | | | | |
| **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** |  | | | |

#### **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** |  | | | |
| **Observations** |  | | | |
| **CCSS Committee Decisions** |  | | | |
| **Inspections** |  | | | |
| **Documents** |  | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | |
| No Level II Requirements | | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | |
| No Level III Requirements | | | | | |

### Aspect 1.02: Wallet Creation

*This aspect covers the creation of wallets or addresses that can receive digital assets. Wallets are created using key signing methodologies that can require a single key’s signature, multiple keys’ signatures, or a minimum number of signatures from many keys. Furthermore, wallets can be created individually (commonly referred to as JBOK wallets, or “Just a Bunch Of Keys”) or in a deterministic way that allows a set of addresses/key pairs to be created from a single master seed. Security of wallet creation is derived from the integrity of the wallet in the face of various risks such as a lost/stolen/compromised key, and the confidentiality of the wallet that would make it difficult to associate a wallet with a particular actor.*

#### 

#### 

#### **Aspect Control 1.02.1: Multiple keys for signing**

| ***LEVEL I REQUIREMENTS*** | | | | | |
| --- | --- | --- | --- | --- | --- |
| No Level I Requirements | | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | |
| **Requirement** | 1.02.1.1 Any address generated by a wallet must require a minimum of 2 signatures (commonly referred to as a multi-sig wallet) in order to spend funds, where a separate actor holds each signing key. The actors can either be human or system (i.e. two humans, two systems, or one human and one system) but must be separate entities that each manage their own key for the wallet. | | | | |
| **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** |  | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | |
| No Level III Requirements | | | | | |

#### **Aspect Control 1.02.2: Redundant key for recovery**

| ***LEVEL I REQUIREMENTS*** | | | | | |
| --- | --- | --- | --- | --- | --- |
| No Level I Requirements | | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | |
| **Requirement** | 1.02.2.1 Redundant keys are assigned to each wallet for recovery purposes. | | | | |
| **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** |  | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | |
| No Level III Requirements | | | | | |

#### **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** |  | | | |
|  | | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | |
| No Level III Requirements | | | | | |

#### **Aspect Control 1.02.4: Organizational distribution of keys**

| ***LEVEL I REQUIREMENTS*** | | | | | |
| --- | --- | --- | --- | --- | --- |
| No Level I Requirements | | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | |
| No Level II Requirements | | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | |
| **Requirement** | 1.02.4.1 Any keys that have signing authority on a single wallet must be stored by multiple organizational entities/business units. | | | | |
| **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** |  | | | |

#### **Aspect Control 1.02.5: Documented wallet creation policy**

| ***LEVEL I REQUIREMENTS*** | | | | | |
| --- | --- | --- | --- | --- | --- |
| No Level I Requirements | | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | |
| **Requirement** | 1.02.5.1 The organization has a documented custody policy in place which details the company’s internal policies and procedures and covers the relevant areas of wallet creation. | | | | |
| **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** |  | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | |
| No Level III Requirements | | | | | |

### Aspect 1.03: Key Storage

*By separating the wallet’s keys across multiple locations, the risks associated with localized disruptions to business (e.g., fire, flood, earthquake, break-ins) do not affect the organization’s ability to spend funds.*

#### **Aspect Control 1.03.1: Primary keys are stored encrypted**

| ***LEVEL I REQUIREMENTS*** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Requirement** | 1.03.1.1 Cryptographic keys and/or seeds must be stored with the use of strong encryption when not in use. | | | | |
| **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** |  | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | |
| No Level II Requirements | | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | |
| No Level III Requirements | | | | | |

#### 

#### 

#### **Aspect Control 1.03.2: Backup key exists**

| ***LEVEL I REQUIREMENTS*** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement** | 1.03.2.1 A backup of the cryptographic key/seed must exist. The backup can take any form (e.g., paper, digital). | | | | | |
| **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** |  | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | | |
| **Requirement** | 1.03.2.2 A backup must exist for at least as many keys as are required to spend funds. | | | | | |
| **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** |  | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | | |
| No Level III Requirements | | | | | | |

#### **Aspect Control 1.03.3: Backup key has environmental protection**

| ***LEVEL I REQUIREMENTS*** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement** | 1.03.3.1 The backup must be protected against environmental risks such as fire, flood, and other acts of God. | | | | | |
| **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** |  | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | | |
| **Requirement** | 1.03.3.2 The backup key/seed must be stored in a location that is geographically separate from the usage location of the primary key/seed. For example, if the primary key is kept at an office, the backup key could be in escrow with a trusted 3rd party. | | | | | |
| **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** |  | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | | |
| **Requirement** | 1.03.3.3 Backups are resistant to electromagnetic pulses that could induce currents in electronics and damage the data stored within. A common methodology to secure against this risk is to store a seed or key on paper, wood, metal, or on another non-digital medium, or to place the digital medium within a sealed faraday bag designed to protect contents from electro-magnetic interference. | | | | | |
| **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** |  | | | | |

#### **Aspect Control 1.03.4: Backup key is access-controlled**

| ***LEVEL I REQUIREMENTS*** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Requirement** | 1.03.4.1 The backup must be protected by access controls that prevent unauthorized parties from accessing it. | | | | |
| **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** |  | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | |
| No Level II Requirements | | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | |
| No Level III Requirements | | | | | |

#### **Aspect Control 1.03.5: Backup key has tamper-evident seal**

| ***LEVEL I REQUIREMENTS*** | | | | | |
| --- | --- | --- | --- | --- | --- |
| No Level I Requirements | | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | |
| **Requirement** | 1.03.5.1 The backup must employ some form of tamper evident mechanism that allows an operator to determine if it has been accessed. | | | | |
| **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** |  | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | |
| No Level III Requirements | | | | | |

#### 

#### 

#### **Aspect Control 1.03.6: Backup key is encrypted**

| ***LEVEL I REQUIREMENTS*** | | | | | |
| --- | --- | --- | --- | --- | --- |
| No Level I Requirements | | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | |
| No Level II Requirements | | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | |
| **Requirement** | 1.03.6.1 Backups of cryptographic keys and/or seeds must be stored with the use of strong encryption when not in use that is at least equal to the security prescribed for cryptographic keys/seeds above. | | | | |
| **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** |  | | | |

### Aspect 1.04: Key Usage

This aspect covers the use of cryptographic keys and/or seeds to ensure they are used in a secure manner that minimizes the risks to the confidentiality of private keys and integrity of funds. This section does not cover the usage of key backups which are only used in the event the primary key is lost/damaged/inaccessible. A variety of risks are present when using keys that can lead to the loss of funds including dirty signature vulnerabilities (i.e. re-used ‘R’ values), opportunity for malware to copy or modify keys, and malicious insiders who use their authorized access to send unauthorized transactions.

#### **Aspect Control 1.04.1: Key access requires user/pass/nth factor**

| ***LEVEL I REQUIREMENTS*** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement** | 1.04.1.1 Access to the primary key/seed requires an identifier (e.g. username, email, GUID, etc.) and at least 2 (two) other factors of authentication, which restricts access to the authorized operator. | | | | | |
| **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** |  | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | | |
| No Level II Requirements | | | | | | |
|  | | | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | | |
| **Requirement** | 1.04.1.2 Access to the key/seed requires an identifier (e.g., username, email, GUID) and at least 3 (three) other factors of authentication. | | | | | |
| **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** |  | | | | |

#### **Aspect Control 1.04.2: Keys are only used in a trusted environment**

| ***LEVEL I REQUIREMENTS*** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Requirement** | 1.04.2.1 All keys/seeds are only used in trusted environments. | | | | |
| **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** |  | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | |
| No Level II Requirements | | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | |
| No Level III Requirements | | | | | |

#### **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** |  | | | |
| **Observations** |  | | | |
| **CCSS Committee Decisions** |  | | | |
| **Inspections** |  | | | |
| **Documents** |  | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | |
| No Level II Requirements | | | | | |
|  | | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | |
| No Level III Requirements | | | | | |

#### **Aspect Control 1.04.4: Operator ID checks**

| ***LEVEL I REQUIREMENTS*** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Requirement** | 1.04.4.1 All key/seed holders (individuals and organizations) have undergone identity verification to ensure they are who they say they are. | | | | |
| **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** |  | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | |
| No Level II Requirements | | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | |
| No Level III Requirements | | | | | |

**Aspect Control 1.04.5: Operator background checks**

| ***LEVEL I REQUIREMENTS*** | | | | | |
| --- | --- | --- | --- | --- | --- |
| No Level I Requirements | | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | |
| No Level II Requirements | | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | |
| **Requirement** | 1.04.5.1 All individual key/seed holders have had background checks performed by law enforcement personnel or investigative firms. | | | | |
| **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** |  | | | |

#### **Aspect Control 1.04.6: Spends are verified before signing**

| ***LEVEL I REQUIREMENTS*** | | | | | |
| --- | --- | --- | --- | --- | --- |
| No Level I Requirements | | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | |
| **Requirement** | 1.04.6.1 Verification of fund destinations and amounts is performed via Approved Communication Channels prior to key/seed use. | | | | |
| **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** |  | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | |
| No Level III Requirements | | | | | |

#### **Aspect Control 1.04.7: No two keys are used on one device**

| ***LEVEL I REQUIREMENTS*** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Requirement** | 1.04.7.1 No two master keys/seeds of the same multi-signature wallet are ever present on the same device. | | | | |
| **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** |  | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | |
| No Level II Requirements | | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | |
| No Level III Requirements | | | | | |

#### 

#### 

#### **Aspect Control 1.04.8: DRBG Compliance**

| ***LEVEL I REQUIREMENTS*** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Requirement** | 1.04.8.1 Digital signatures must use a ‘k’ value that is never repeated. | | | | |
| **Audit Finding Summary** | **In-Place** | **In-Place with Comparable Control** | **Qualified for In-Place** | **Not In-Place** | **Not Applicable** |
| ☐ | ☐ | ☐ | ☐ | ☐ |
| **CCSSA Findings** | A “k” value is generated on the platform which creates the digital signature. For all digital signatures created on the [ENTITY] systems Intel’s RDRAND interface which is compliant with NIST SP 800-90A is used. | | | | |
| **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** |  | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | |
| No Level II Requirements | | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | |
| No Level III Requirements | | | | | |

### Aspect 1.05: Key Compromise Policy

*This aspect covers the existence and use of a protocol that dictates the actions that must be taken in the event a cryptographic key/seed or its operator/holder is believed to have become compromised. Organizations must be prepared to deal with a situation where a private key has – even potentially – become known, determinable, or destroyed. Proper policies and procedures to govern these events decrease the risks associated with lost funds and disclosed trade secrets, and increase the availability of the information system to its users. Examples of when a KCP would be invoked include the identification of tampering of a tamper-evident seal placed on key material, the apparent disappearance of an operator whose closest friends and family cannot identify their whereabouts, or the receipt of communication that credibly indicates an operator or key is likely at risk of being compromised. The execution of Key Compromise Protocols must make use of Approved Communication Channels to ensure KCP messages are only sent/received by authenticated actors.*

#### **Aspect Control 1.05.1: KCP Exists**

| ***LEVEL I REQUIREMENTS*** | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Requirement** | 1.05.1.1 An inventory of all keys/seeds exists and the organization has an awareness of which keys are critical to the successful operation of the information system. | | | | | | |
| **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** |  | | | | | |
| **Requirement** | 1.05.1.2 While no formal KCP documents may exist, there is a staff member who is able to direct operators in the procedures necessary to regenerate cryptographic keys, regenerate cryptocurrency wallets, and send funds to these newly-generated wallets in the event any operator or keys become compromised. | | | | | | |
| **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** |  | | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | | | |
| **Requirement** | 1.05.1.3 A Key Compromise Protocol is documented which details: each specific classification of key used throughout the system; a detailed plan of dealing with its compromise that includes the use of Approved Communication Channels during execution; identities of actors via roles (not names), and includes secondary actors in the event any primary actor is unavailable to carry out the KCP. | | | | | | |
| **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** |  | | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | | | |
| No Level III Requirements | | | | | | | |

#### **Aspect Control 1.05.2: KCP Training and Rehearsals**

| ***LEVEL I REQUIREMENTS*** | | | | | |
| --- | --- | --- | --- | --- | --- |
| No Level I Requirements | | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | |
| No Level II Requirements | | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | |
| **Requirement** | 1.05.2.1 The Key Compromise Protocol is tested periodically to confirm the viability of the procedures and to ensure staff remain trained to use them in the case of a compromise. Logs of executed tests exist which outline any/all comments of the test. Improvements identified during the tests are written back into the protocol to ensure the most effective and efficient protocol is always maintained. As changes are made to the information system, the Key Compromise Protocol is revisited to assure it is updated with any new class of key. | | | | |
| **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** |  | | | |

### Aspect 1.06: Keyholder Grant/Revoke Policies and Procedures

*This aspect covers the policies and procedures surrounding granting and revoking access to cryptographic keys or seeds that store organizational or end-user funds. Staff typically have greater access to an information system with respect to accessing its information, invoking privilege-restricted actions, and representing the organization to the public. Improper management of the onboarding and offboarding of personnel introduce risks of privileged accounts remaining when staff depart, as well as unrevoked keys that persist signing authority for certain transactions.*

#### **Aspect Control 1.06.1: Grant/Revoke Procedures/Checklist**

| ***LEVEL I REQUIREMENTS*** | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Requirement** | 1.06.1.1 An awareness of how roles should be managed when onboarding or offboarding staff from keyholder positions exists within the organization. A staff member who is knowledgeable about the system is able to ensure that permissions are granted/revoked to/from the affected staff appropriately. | | | | | | |
| **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** |  | | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | | | |
| **Requirement** | 1.06.1.2 The organization maintains checklists that cover all tasks that must be completed when staff vacate or transition into keyholder roles within the organization. These checklists have been reviewed by knowledgeable personnel to ensure “least privilege principles” are applied to the information system, as well as necessary access where required. | | | | | | |
| **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** |  | | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | | | |
| No Level III Requirements | | | | | | | |

#### **Aspect Control 1.06.2: Requests made via Approved Communication Channel**

| ***LEVEL I REQUIREMENTS*** | | | | | |
| --- | --- | --- | --- | --- | --- |
| No Level I Requirements | | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | |
| **Requirement** | 1.06.2.1 All keyholder grant/revoke requests are conducted over Approved Communication Channels. | | | | |
| **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** |  | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | |
| No Level III Requirements | | | | | |

#### 

#### 

#### **Aspect Control 1.06.3: Grant/Revoke Audit Trail**

| ***LEVEL I REQUIREMENTS*** | | | | | |
| --- | --- | --- | --- | --- | --- |
| No Level I Requirements | | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | |
| No Level II Requirements | | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | |
| **Requirement** | 1.06.3.1 The organization’s checklists include auditing information that records the identity of the staff member that performs the grant/revoke operations. Each entry within the audit trail is attested to by the staff member who performed that task. | | | | |
| **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** |  | | | |

## Operations

### Aspect 2.01: Security Tests / Audits

*This aspect covers third-party reviews of the security systems, technical controls, and policies that protect the information system from all forms of risk as well as vulnerability and penetration tests designed to identify paths around existing controls. Regardless of the technical skills, knowledge, and experience of staff who build and maintain an information system, it has been proven that third-person reviews often identify risks and control deficiencies that were either overlooked or underestimated by staff. For the same reasons that development companies require different people to test a product from those who write it, different people than those who implement a cryptocurrency system should assess its security. Third parties provide a different viewpoint and are independent of the technical controls and can be objective without risk of retaliation.*

#### 

#### **Aspect Control 2.01.1: Security Audit**

| ***LEVEL I REQUIREMENTS*** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement** | 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. | | | | | |
| **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** |  | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | | |
| **Requirement** | 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 organization. | | | | | |
| **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** |  | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | | |
| **Requirement** | 2.01.1.3 A regular security audit at a level similar to SOC2, ISAE3402, or ISO-27001, that includes vulnerability, penetration testing, and code audit (if applicable) 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 organization, and known vulnerabilities have been removed from the system. Ongoing audits are scheduled on a (minimum) yearly basis. | | | | | |
| **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** |  | | | | |

### Aspect 2.02: Data Sanitization Policy

*This aspect covers the removal of cryptographic keys from digital media. Due to the manner in which file systems allocate data on digital media, digital forensic techniques can be employed to read old data that has previously been deleted. Proper sanitization of digital media ensures the proper removal of all keys, eliminating the risk of information leakage from decommissioned devices like servers, hard disk drives, and removable storage.*

#### **Aspect Control 2.02.1: DSP Exists**

| ***LEVEL I REQUIREMENTS*** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement** | 2.02.1.1 The organization’s staff is aware of how data persists on digital media after deletion. Staff also have access to tools that perform secure deletion of data and understand when to use such tools to permanently destroy any transient copies of cryptographic keys that may be required during the maintenance of the information system. | | | | | |
| **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** |  | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | | |
| **Requirement** | 2.02.1.2 A detailed policy that aligns to NIST 800-88 by outlining the requirements for sanitization of digital media that holds/held cryptocurrency keys exists is read/understood by all staff who have access to cryptographic keys. Procedure documents outline where sanitization is required in their processes. | | | | | |
| **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** |  | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | | |
| No Level III Requirements | | | | | | |

#### **Aspect Control 2.02.2: Audit Trail of all media sanitization**

| ***LEVEL I REQUIREMENTS*** | | | | | |
| --- | --- | --- | --- | --- | --- |
| No Level I Requirements | | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | |
| No Level II Requirements | | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | |
| **Requirement** | 2.02.2.1 An audit trail is maintained for every piece of sanitized media conforming to the NIST 800-88 recommendation. These audit documents identify the staff member who performed the sanitization, the specific identifiers of the media that was sanitized, which tool and configuration was used to perform the sanitization, and all other relevant pertinent information. | | | | |
| **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** |  | | | |

### Aspect 2.03: Audit Logs

*This aspect covers the information system’s maintenance of audit logs that provide a record of all changes to information throughout the system. In the event of unexpected behavior or security incidents, audit logs are an extremely valuable tool that can help investigators understand how the unexpected symptoms occurred and how to resolve the inconsistencies to return the information system to a consistent state. The maintenance of audit logs significantly reduces the risks associated with operational awareness and increases the information system’s ability to correct any inaccuracies.*

#### **Aspect Control 2.03.1: Application Audit Logs**

| ***LEVEL I REQUIREMENTS*** | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Requirement** | 2.03.1.1 Audit trails exist for a subset of actions that are performed within the information system. | | | | | | |
| **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** |  | | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | | | |
| **Requirement** | 2.03.1.2 All actions by all users are logged. Audit logs are retained for at least 1 year in a trusted environment. | | | | | | |
| **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** |  | | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | | | |
| No Level III Requirements | | | | | | | |

#### **Aspect Control 2.03.2: Backup of Audit Logs**

| ***LEVEL I REQUIREMENTS*** | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| No Level I Requirements | | | | | | | |
| ***LEVEL II REQUIREMENTS*** | | | | | | | |
| **Requirement** | 2.03.2.1 In addition to recording all actions performed within the system, this audit information is **periodically** backed up to a separate server. | | | | | | |
| **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** |  | | | | | |
| ***LEVEL III REQUIREMENTS*** | | | | | | | |
| **Requirement** | 2.03.2.2 In addition to recording all actions performed within the system, this audit information is **continually** backed up to a separate server. | | | | | | |
| **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** |  | | | | | |

# Audit Evidence

## Interviews Conducted [INTERVIEW]

| **Reference Number** | **Topics Covered in Interviews** | **Interviewee Name** | **Interviewee Role** | **Interviewee Organization** |
| --- | --- | --- | --- | --- |
|  | Key management processes, cryptographic formulas used… |  |  |  |

## Documentation Reviewed [DOCUMENT]

| **Reference Number** | **Document Name** | **Description of Document Purpose** | **Document Revision Date (if applicable)** |
| --- | --- | --- | --- |
|  |  |  |  |

## Process Observations [OBSERVATION]

| **Reference Number** | **Process Observed** | **Description of What Was Observed** | **Date Observed** |
| --- | --- | --- | --- |
|  |  |  |  |

## Inspections [INSPECTION]

| **Reference Number** | **What Was Inspected** | **Inspection Findings** | **Date Inspected** |
| --- | --- | --- | --- |
| INSPECTION\_1 |  |  |  |

## CCSS Committee Decisions [CCSS\_DECISION]

If the assessed entity provides evidence that the CCSSA needs to seek guidance from the CCSS Committee as to its validity for inclusion as evidence then the details of the evidence presented, comments by the CCSSA and comments by a CCSS Committee member are documented in this section.

| **Reference Number** | **Evidence Presented** | **Date of CCSS Committee Decision** | **CCSSA Comments** | **CCSS Committee Comments** |
| --- | --- | --- | --- | --- |
| CCSS\_DECISION\_1 |  |  |  |  |

Disclaimer

The CCSSA who performed this report has based the findings of the specific evidence observed at the time of the audit. This does not guarantee evidence of future performance of any of the requirements.

Any significant changes to the security practices and procedures that occur by the audited entity could invalidate the audit and must be disclosed to the CCSSA in a timely manner.

Note

C4 would like to thank Confide Limited for developing this template for use with the CCSS. Special thanks to CCSSA Marc Krisjanous for compiling this RoC template.

**DOCUMENT END**