



CCSS Foundations Course

Build the knowledge to read, interpret, and discuss CCSS with confidence.

12 HOURS

LIVE, INSTRUCTOR-LED

INTERACTIVE & APPLIED

Course overview

The CCSS Foundations Course provides a detailed guide to the Cryptocurrency Security Standard and the security thinking behind it and how it helps protect cryptocurrency and digital asset systems. This course helps participants understand how CCSS is organized, why its requirements exist, and how they relate to the real-world protection of cryptocurrency systems.

What you'll learn

- How CCSS is structured, including its categories, aspects, controls, requirements, terminology, and certification levels
- How to distinguish an entity from the cryptocurrency system being evaluated and define the CCSS Trusted Environment
- How risks develop across the cryptographic key lifecycle—from generation and wallet creation through storage, access, usage, and sanitization
- How operational controls such as testing, logging and monitoring, governance, risk management, and key-compromise planning support secure operations
- How the different CCSS levels compare and what changes as requirements become more rigorous
- How certification works and how Implementers, Auditors, Peer Reviewers, C4, and Entities fit into the CCSS ecosystem

What happens during the training

- Ask questions throughout the course and discuss challenging concepts directly with the instructor and other learners
- Work through CCSS glossary terms and use the Standard's terminology in context
- Examine specific wording in requirements and discuss why subtle differences in language can change interpretation
- Compare requirements across CCSS levels and discuss the practical significance of those differences

- Participate in group discussions and activities using examples and real security incidents
- Complete quizzes and knowledge checks that reinforce key concepts and surface areas for additional discussion

What you'll walk away with

- A working vocabulary for discussing CCSS with technical, security, risk, and compliance teams
- A clearer understanding of the relationships among scope, risk, key management, operations, and certification
- The foundation needed to continue into the more applied CCSS Implementer or CCSS Auditor training pathways

Skills that extend beyond the CCSS

While CCSS provides the framework for the course, the skills developed extend well beyond a single standard. Participants strengthen their ability to scope complex systems, identify trust boundaries, evaluate threats and risk, question assumptions, interpret security requirements, assess the effectiveness of controls, and communicate security issues across technical and non-technical teams.

For security leaders and decision makers, the course also provides a framework for asking better questions and understanding not only whether a control exists, but what risk it addresses, how it works, how its effectiveness is demonstrated, and what could happen if it fails.

Foundations: Develops the ability to understand and discuss cryptocurrency security risk intelligently across technical, operational, governance, and business teams.

Implementer: Develops structured problem-solving skills for moving from identified risk to practical, documented, and defensible security improvements.

Auditor: Develops critical evaluation skills for distinguishing assertions from evidence and reaching conclusions that can withstand independent scrutiny.



CCSS Implementer Course

Learn a repeatable methodology for turning CCSS requirements into practical security improvements.

12 HOURS

LIVE, INSTRUCTOR-LED

INTERACTIVE & APPLIED

Course overview

The CCSS Implementer (CCSSI) Course focuses on the work required to move from understanding the Standard to applying it. Participants learn how to evaluate a cryptocurrency system, establish scope, identify gaps and risks, and translate CCSS requirements into practical improvements that can be documented and prepared for independent audit.

What you'll learn

- How to begin an implementation engagement and gather the information needed to understand the system
- How to define system boundaries and map the CCSS Trusted Environment across people, processes, technology, and dependencies
- How to conduct a gap assessment against applicable CCSS requirements and organize remediation priorities
- How system diagrams support scoping, threat modeling, risk assessment, and implementation decisions
- How threat modeling approaches such as STRIDE, OWASP, and MITRE ATT&CK can be used to identify credible attack paths
- How to assess risk and use it to prioritize security improvements
- How to translate CCSS requirements into policies, procedures, technical controls, documentation, and evidence

What happens during the training

- Ask implementation questions and discuss alternative approaches with the instructor and other participants
- Work through CCSS terminology, Levels, and the nuances of requirement language from an implementer's perspective
- Participate in group activities that require scoping systems, identifying gaps, considering threats, and making implementation decisions
- Apply concepts to a fictional cryptocurrency custody environment, rather than working only from abstract examples in a mock implementation.

- Discuss where multiple implementation approaches may satisfy the objective of a requirement and what must still be demonstrated
- Complete knowledge checks throughout the training to reinforce concepts and identify areas needing clarification

Why instructor-led training matters

An Implementer needs more than a checklist. The value of the course is learning how to connect system understanding, scope, threat modeling, risk, gap analysis, remediation, documentation, and audit readiness. Participants practice the judgment involved in deciding what information is missing, what needs to change, and how to build an implementation that can later be independently assessed.

What you'll walk away with

- A structured methodology for approaching a CCSS implementation engagement
- Practice applying CCSS concepts to an imperfect, realistic system scenario
- A clearer understanding of how to move from a requirement to an implementable and auditable control environment
- A practical view of the boundary between implementation assistance and the independent Auditor's role
- Greater confidence in your CCSSI exam preparation, supported by a deeper understanding of CCSS requirements and experience applying them to realistic implementation scenarios.

Skills that extend beyond the CCSS

While CCSS provides the framework for the course, the skills developed extend well beyond a single standard. Participants strengthen their ability to scope complex systems, identify trust boundaries, evaluate threats and risk, question assumptions, interpret security requirements, assess the effectiveness of controls, and communicate security issues across technical and non-technical teams.

For security leaders and decision makers, the course also provides a framework for asking better questions and understanding not only whether a control exists, but what risk it addresses, how it works, how its effectiveness is demonstrated, and what could happen if it fails.

Foundations: Develops the ability to understand and discuss cryptocurrency security risk intelligently across technical, operational, governance, and business teams.

Implementer: Develops structured problem-solving skills for moving from identified risk to practical, documented, and defensible security improvements.

Auditor: Develops critical evaluation skills for distinguishing assertions from evidence and reaching conclusions that can withstand independent scrutiny.



CCSS Auditor Course

Develop the judgment to evaluate evidence, challenge assumptions, and support defensible CCSS audit conclusions.

12 HOURS

LIVE, INSTRUCTOR-LED

INTERACTIVE & APPLIED

Course overview

The CCSS Auditor (CCSSA) Course focuses on independently evaluating whether a cryptocurrency system meets the Standard. Participants follow the audit lifecycle from engagement and scope through evidence collection, testing, documentation, reporting, peer review, and certification submission, with emphasis on the professional judgment required to reach supportable conclusions.

What you'll learn

- How a CCSS audit progresses from engagement, Intent to Audit, and scope through fieldwork, reporting, peer review, and certification
- How to evaluate audit readiness and determine whether the system and available evidence are ready for formal assessment
- How auditor independence affects the engagement and where implementation assistance can create conflicts
- How to test requirements using interviews and evidence review, including review, inspection, and observation
- How to evaluate evidence across cryptographic asset management and operational security requirements
- How differences between CCSS Levels and nuances in requirement language affect testing and conclusions
- How to document exceptions, remediation, retesting, and conclusions and prepare the RoC, redacted RoC, SROc, and peer-review materials

What happens during the training

- Ask audit and interpretation questions throughout the course and discuss difficult evidence scenarios with the instructor
- Work through glossary terms and requirement wording from an auditor's perspective, including language that changes what must be evidenced
- Compare CCSS Levels and discuss how the level being assessed changes the audit expectation
- Use a fictional centralized cryptocurrency exchange, to practice reviewing a system rather than discussing auditing only in theory during a mock audit.
- Participate in group activities involving scope, evidence evaluation, follow-up questions, findings, and supportable conclusions



CRYPTOCURRENCY SECURITY STANDARD

Training

- Complete knowledge checks that reinforce audit concepts and identify areas requiring additional discussion

Why instructor-led training matters

Auditing CCSS is not a matter of deciding whether a requirement sounds satisfied. Participants learn to ask what evidence supports the conclusion, whether that evidence is sufficient, what additional testing is needed, and whether another qualified reviewer could follow the audit trail. The course gives participants practice in the judgment that is difficult to develop by reading the Standard alone.

What you'll walk away with

- A practical understanding of the end-to-end CCSS audit and certification workflow
- A stronger framework for evaluating evidence and documenting defensible conclusions
- Practice identifying gaps, asking better follow-up questions, and distinguishing assertion from audit evidence
- An understanding of how peer review tests the quality and supportability of completed audit work
- Greater confidence in your CCSSA exam preparation, supported by practice interpreting CCSS requirements, evaluating evidence, and applying audit concepts to realistic scenarios.

Skills that extend beyond the CCSS

While CCSS provides the framework for the course, the skills developed extend well beyond a single standard. Participants strengthen their ability to scope complex systems, identify trust boundaries, evaluate threats and risk, question assumptions, interpret security requirements, assess the effectiveness of controls, and communicate security issues across technical and non-technical teams.

For security leaders and decision makers, the course also provides a framework for asking better questions and understanding not only whether a control exists, but what risk it addresses, how it works, how its effectiveness is demonstrated, and what could happen if it fails.

Foundations: Develops the ability to understand and discuss cryptocurrency security risk intelligently across technical, operational, governance, and business teams.

Implementer: Develops structured problem-solving skills for moving from identified risk to practical, documented, and defensible security improvements.



Auditor: Develops critical evaluation skills for distinguishing assertions from evidence and reaching conclusions that can withstand independent scrutiny.