TrustCrypto Certified Compliance Specialist (TCCS)

Examination Syllabus

Version: 2.4

Effective: 1 January 2026

Next Review: Q3 2026

Purpose

The TrustCrypto Certified Compliance Specialist (TCCS) credential is designed for professionals responsible for crypto-related compliance, risk assessment, and financial crime prevention.

The certification assesses competence in applying published standards to compliance scenarios, with particular emphasis on AML/KYC frameworks, blockchain forensics, regulatory reporting, and defensible risk assessment.

TCCS is not a teaching qualification. It is an assessment of professional competence against the TrustCrypto Standards Framework v1.0.

Target Professional Roles

The TCCS examination is designed for:

- Compliance officers in firms handling cryptoassets
- Risk and governance professionals assessing crypto exposure
- Accountants and auditors reviewing crypto holdings
- Legal practitioners advising on crypto regulatory matters
- Financial crime analysts and investigators

TCCS does not confer regulatory permissions. It signals adherence to published professional standards.

Examined Domains

Assessment is structured across five domains. Weightings reflect relative emphasis in the examination.

Domain 1: AML/KYC Frameworks & Controls (25%)

Scope:

- UK Money Laundering Regulations and crypto-specific guidance
- Customer due diligence (CDD) and enhanced due diligence (EDD)
- Beneficial ownership identification and verification
- Politically exposed persons (PEPs) and sanctions screening
- Ongoing monitoring and transaction surveillance
- Record-keeping obligations and evidence standards

Learning Outcomes:

Candidates should be able to:

- Apply AML/KYC frameworks to crypto-specific scenarios
- Design and evaluate customer due diligence procedures
- Identify when enhanced due diligence is required
- Assess compliance with UK Money Laundering Regulations
- Document defensible risk-based decisions

Domain 2: Blockchain Forensics & Transaction Tracing (20%)

Scope:

- Blockchain analysis techniques and limitations
- Transaction tracing across protocols (Bitcoin, Ethereum, etc.)
- Mixer/tumbler identification and cluster analysis
- Exchange attribution and flow analysis
- Evidence collection and chain of custody
- Reporting findings to law enforcement or regulators

Learning Outcomes:

Candidates should be able to:

- Interpret blockchain transaction data for compliance purposes
- Identify common obfuscation techniques and red flags
- Distinguish legitimate privacy from suspicious activity
- Collect and preserve blockchain evidence appropriately
- Communicate findings to non-technical stakeholders

Domain 3: Risk Assessment & Governance Reporting (20%)

Scope:

- Crypto-specific risk categorisation frameworks
- Operational, custody, and protocol risk assessment
- Risk appetite statements and tolerance thresholds
- Escalation triggers and decision frameworks
- Board and senior management reporting
- Regulatory reporting obligations (SARs, STRs, etc.)

Learning Outcomes:

Candidates should be able to:

- Assess and categorise crypto-related risks
- Design proportionate risk assessment frameworks
- Determine when to escalate vs manage within tolerance
- Prepare defensible risk reporting for governance bodies
- Meet regulatory reporting obligations accurately and timely

Domain 4: Regulatory Compliance & Reporting (20%)

Scope:

- FCA cryptoasset regulatory perimeter and guidance
- Registration requirements for crypto businesses (MLRs)
- Travel Rule compliance and cross-border reporting
- MiCA equivalence and EU regulatory alignment
- Suspicious Activity Reports (SARs) and Suspicious Transaction Reports (STRs)
- Regulatory engagement and proactive disclosure

Learning Outcomes:

Candidates should be able to:

- Determine which activities fall within or outside regulatory scope
- Apply FCA guidance to novel crypto products or services
- Prepare compliant regulatory reports and filings
- Assess MiCA implications for cross-border operations
- Engage constructively with regulators when required

Note: Assessment emphasises understanding of compliance frameworks and control principles rather than memorisation of specific guidance references.

Domain 5: Ethics & Professional Conduct (15%)

Scope:

- Conflicts of interest in compliance roles
- Professional independence and objectivity
- Duty to report vs duty of confidentiality
- Whistleblowing protections and obligations
- Professional boundaries and competency limits
- When to seek specialist legal or technical input

Learning Outcomes:

Candidates should be able to:

- Identify and manage conflicts of interest
- Navigate competing obligations (client, employer, regulator)
- Recognise when professional independence is compromised
- Apply ethical frameworks to ambiguous compliance scenarios
- Determine when to escalate or refer matters beyond competency

Assessment Format

The TCCS examination comprises:

- 60 multiple-choice questions (75 minutes)
- 2 written scenario responses (60 minutes)
- Scenario responses: 2 × ~300-400 words each
- Scenario marking: Assessed against a published rubric
- Scenario weighting: 20% of total marks (10% each)

Multiple-choice questions assess knowledge recall and application across all domains. Scenario responses assess applied competence in realistic compliance and investigative contexts.

Professional judgement applies until a defined Institute threshold is met, at which point mandatory duties under the Code of Professional Conduct are triggered, as set out in the Judgement → Duty Guide.

Pass Standard: 70% or higher across all components. Questions are mapped to domain weightings. Not all domains receive equal representation in every examination sitting.

Assessment Principles

Assessment focuses on applied competence. Candidates are expected to demonstrate:

- Working knowledge of relevant legislation and guidance
- Ability to apply published standards to realistic advisory scenarios
- Professional judgement appropriate to the role

Candidates are not expected to:

- Memorise specific regulation references, section numbers, or dates
- Provide specialist legal or tax advice beyond the advisory role
- Demonstrate technical blockchain development or coding skills

Standards Framework Reference

All examination content is derived from the TrustCrypto Standards Framework v1.0.

The Standards Framework defines:

- Professional conduct expectations
- Technical competency baselines
- Compliance and risk management principles
- Regulatory alignment requirements

Candidates are expected to demonstrate familiarity with the Standards Framework and ability to apply its principles to novel situations.

The Standards Framework is available at: https://trustcrypto.co.uk/standards

CPD Hours

Successful candidates are awarded 40 CPD hours upon passing the TCCS examination.

CPD hours are awarded for assessment completion, not for study time. Hours are not awarded for unsuccessful attempts or participation without certification.

Certification Validity & Renewal

TCCS certification is issued with an expectation of ongoing standards alignment. The Institute does not currently mandate time-limited renewal, but reserves the right to implement renewal requirements to ensure continued professional currency.

Certificate status may be:

- Active: In good standing
- Lapsed: Renewal requirements not met (if introduced)
- Revoked: Removed due to misconduct or material breach

Public verification is available via the TrustCrypto registry.

Study Approach

The Institute does not provide mandatory training or prescribed study materials.

Candidates are expected to:

- Review the TrustCrypto Standards Framework
- Study TrustCrypto Institute Guides (primary authoritative resources)
- Consult TCCS Reading List v2.6.0 for supplementary materials
- Familiarise themselves with assessment format via indicative examples
- Apply professional judgement to examination preparation

Institute Guides: TrustCrypto Institute Guides are the authoritative reference for examination content. All marking criteria and model answers are derived from Institute frameworks. External materials are supplementary and provided for contextual understanding only.

The syllabus defines scope. Candidates are responsible for achieving competency within that scope.

Policy References

Examination governance: https://trustcrypto.co.uk/exams

Examination policies: https://trustcrypto.co.uk/exams/policies

Standards Framework: https://trustcrypto.co.uk/standards

Reading List: https://trustcrypto.co.uk/tccs/reading-list

Contact

Syllabus enquiries: syllabus@trustcrypto.co.uk

TrustCrypto Institute

Version 2.4 | Effective 1 January 2026 | Next Review Q3 2026