



Crypto audit readiness checklist: what the auditor asks for, and what a good answer looks like

Ten requests that come up in almost every audit of crypto holdings. Each item states what the auditor will ask for and what a good answer looks like, so you can close the gaps before fieldwork rather than during it.

Work through it at least a month before the audit starts.

CryptaCount

www.cryptacount.com

General information, not accounting, legal or tax advice

Crypto audit readiness checklist: what the auditor asks for, and what a good answer looks like

Ten requests that come up in almost every audit of crypto holdings. Each item states **what the auditor will ask for** and **what a good answer looks like**, so you can close the gaps before fieldwork rather than during it. Work through it at least a month before the audit starts.

The shape of a crypto audit

An auditor testing digital assets is answering four questions: does the entity control what it says it controls, is the transaction population complete, are the numbers measured on a documented and consistently applied basis, and can any posted figure be traced back to source. Everything below serves one of those four. Where an entity fails, it is usually on completeness or on transfers, not on arithmetic.

The checklist

1. Wallet and exchange inventory, with proof of control

Asked for: a complete register of every wallet address, exchange account and custodial relationship in scope at period end, plus evidence that the entity controls each one. **A good answer:** a maintained register naming each address or account, the chain or venue, the purpose, the responsible signatories, and the control evidence, such as a signed message from the address, a small controlled transfer, or custodian confirmation. Include addresses opened and closed during the period, not just those live at the reporting date.

2. Completeness of the transaction population

Asked for: evidence that every transaction in the period has been captured, not just those the accounting team knew about. **A good answer:** the population is derived from the wallet register itself, pulled directly from chain data and exchange APIs rather than from manual exports, with a documented reconciliation of opening balance plus movements to closing balance for each address. Any address in the register that produced no data should be explained, not silently omitted.

3. Internal transfers not treated as disposals

Asked for: a listing of movements between the entity's own wallets and evidence that none of them produced a realised gain or loss. **A good answer:** each internal transfer is matched outflow to inflow, both legs sit inside the wallet register, carrying amount is carried across, and the report shows zero gain on those movements. This is the highest-yield test an auditor runs, because a transfer booked as a sale creates a gain that never existed and inflates both the income statement and the tax position.

4. Cost-basis method, documented and consistently applied

Asked for: the method chosen, where it is documented, and proof that it was applied to every disposal without exception. **A good answer:** the method is named in the signed accounting policy, it is enforced by the system rather than by the preparer, and a re-run over the same data reproduces the same gains. Note that a change in method mid-period, or a different method used in one wallet, is a finding in itself.

5. Fair-value convention

Asked for: which price source was used, at which cut-off, and what happened for assets the source did not cover. **A good answer:** a documented source or hierarchy, a fixed cut-off time and time zone applied at every period end, a stated fallback for missing prices, and stored prices with their timestamps so the auditor can reproduce a valuation rather than accept it.

6. Lot-level workings behind each gain or loss

Asked for: for a sample of disposals, the specific acquisition lots consumed, their basis, the proceeds and the resulting gain or loss. **A good answer:** a per-lot ledger that shows, for the sampled disposal, exactly which lots were relieved and why the method selected them, with the arithmetic visible. A summary figure with no lot detail behind it cannot be tested and will be treated as unsupported.

7. Sub-ledger to general ledger reconciliation

Asked for: proof that the postings in the general ledger agree to the detail in the crypto sub-ledger, and that the asset balances on the books equal the holdings actually on chain and at exchanges at the cut-off. **A good answer:** a period reconciliation with each summarised GL line decomposing into its underlying transactions, and any difference explained by cause, for example a late-syncing wallet or an unclassified transaction, rather than by a balancing adjustment.

8. Treatment and classification of fees

Asked for: how acquisition fees, disposal fees and network fees were treated, and whether the treatment matches the stated policy. **A good answer:** acquisition fees traceable into cost basis,

disposal fees traceable into net proceeds, network fees classified per policy, and the native-token disposal arising on gas settlement recognised rather than ignored. Fees handled inconsistently distort both the balance sheet and realised gains.

9. The signed accounting policy

Asked for: the crypto accounting policy in force during the period, signed and dated. **A good answer:** a current, approved document covering scope, framework, measurement basis, cost-basis method, fair-value convention, fee treatment, income treatment and internal transfers, with superseded versions retained so the auditor can see which applied when. If you do not have one, start from the [crypto accounting policy template](#).

10. An audit trail that supports re-performance

Asked for: take one posted journal entry and trace it back to source. **A good answer:** the summarised GL entry points to its component transactions, each transaction points to a wallet, an exchange fill or an on-chain transaction hash, and the price used points to a stored, timestamped quote. The auditor should be able to re-perform the posting end to end without asking the finance team to reconstruct anything by hand.

Quick self-assessment

Item	Evidence to have ready	Status
Wallet and account register	Full list with proof of control per address or account.	
Completeness	Population derived from the register, balances rolled forward and agreed.	
Internal transfers	Matched legs, carrying amount preserved, zero gain reported.	
Cost-basis method	Named in policy, system enforced, reproducible on re-run.	
Fair-value convention	Source, cut-off, fallback, and stored timestamped prices.	
Lot-level workings	Per-lot detail behind every posted gain or loss.	
Sub-ledger to GL	Period reconciliation with differences explained by cause.	
Fees	Acquisition, disposal and network fees traced to policy treatment.	
Accounting policy	Signed, dated, version controlled, in force for the period.	
Audit trail	Posting traceable to transaction hash or exchange fill and stored price.	

Closing the gaps

Most of this checklist is a system problem rather than an effort problem. A [crypto sub-ledger](#) holds the wallet register, pulls the population directly from chain and venue data, recognises own-wallet movements as internal transfers, applies one cost-basis method deterministically, stores the prices it used, and keeps every summarised posting linked to the transactions and hashes beneath it.

CryptaCount covers 90+ blockchain networks and 100+ exchange and wallet connectors, with IFRS and US GAAP ledgers, so the evidence exists as a by-product of the close rather than as a project before the audit.

Disclaimer. General information, not legal, accounting or tax advice. Audit expectations vary by auditor and framework, confirm requirements with your auditor and a qualified advisor.



Put your crypto books on a real sub-ledger at app.cryptacount.com

© 2026 CryptaCount. All rights reserved.