

Testing checklist: crypto exchange

Source: <https://howtotestaproduct.com/how-to-test/crypto-exchange/>

Generated: 2026-10-07. Licence: CC BY 4.0.

☐ 1. release smoke tests

Done when: After each deploy, a test account places, fills and cancels a small order on web and mobile, and the balance and order history match.

Risks: outage-under-load, store-rejection. Tool class: browser automation. Usually run by: QA engineer.

☐ 2. compliance checks

Done when: Test deposits that match monitoring scenarios raise alerts that reach the review queue, and sign-ups from unlicensed countries are blocked in app and on web.

Risks: regulatory-penalty, fraud-abuse, store-rejection. Tool class: test management. Usually run by: product manager.

☐ 3. end-to-end functional tests

Done when: A withdrawal to a new address after a password or phone change triggers a hold and an email the account owner must confirm.

Risks: fraud-abuse, money-loss. Tool class: browser automation. Usually run by: QA engineer.

☐ 4. penetration testing

Done when: An external tester cannot approve a withdrawal from the hot or multisig wallet without the required signers, and cannot read another customer's account from the support console.

Risks: money-loss, data-breach. Tool class: proxy. Usually run by: security specialist.

☐ 5. unit tests

Done when: Margin, liquidation and fee rules return the expected result for each test case, and no account flag bypasses liquidation without a recorded approval.

Risks: money-loss. Tool class: unit framework. Usually run by: developer.

☐ 6. data integrity and migration testing

Done when: After each ledger close and each wallet movement, customer balances per asset in the ledger sum to no more than on-chain and custodial holdings, and no account other than approved market makers carries a negative balance.

Risks: money-loss. Tool class: data validation. Usually run by: QA engineer.

☐ 7. security scanning

Done when: Each release is scanned and no open high finding remains on withdrawal address changes, API trading keys or stored ID documents.

Risks: data-breach. Tool class: DAST scanner. Usually run by: security specialist.

☐ 8. performance and load testing

Done when: With a replay of the busiest price-spike traffic on record, login, order placement and cancel stay within the agreed response target.

Risks: outage-under-load. Tool class: load generator. Usually run by: developer.

☐ 9. resilience and failure testing

Done when: With one matching engine node or database replica stopped during a load test, orders keep matching and the status page reports degraded service.

Risks: outage-under-load. Tool class: chaos tool. Usually run by: developer.