

Testing checklist: online marketplace

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

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

☐ 1. release smoke tests

Done when: On the release build, a buyer finds a listing, reports it, blocks the seller and completes a purchase from another seller.

Risks: store-rejection. Tool class: mobile automation. Usually run by: QA engineer.

☐ 2. end-to-end functional tests

Done when: A test seller crosses the volume threshold, is asked for verification, and has listings paused until verified; a buyer report on a listing reaches the trust team queue.

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

☐ 3. penetration testing

Done when: A tester signed in as seller A cannot read seller B's buyers, orders or payout account, or change another seller's bank details, by editing ids, and a seller account set up with a tax ID that does not match the seller's verified name cannot receive a payout.

Risks: data-breach, fraud-abuse. Tool class: proxy. Usually run by: security specialist.

☐ 4. compliance checks

Done when: A signed checklist shows that sellers above the volume threshold are verified, and that their name, address and a report link show on every listing on web and app.

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

☐ 5. exploratory testing

Done when: A session log records attempts at fake-seller onboarding, refund abuse, off-platform payment requests in messages and review manipulation, with the platform's response to each.

Risks: fraud-abuse. Tool class: test management. Usually run by: QA engineer.

☐ 6. data integrity and migration testing

Done when: A daily ledger report shows, for every order, buyer charge equal to seller payout plus fees plus refunds, and lists every high-volume seller with verified details.

Risks: regulatory-penalty. Tool class: data validation. Usually run by: QA engineer.

☐ 7. security scanning

Done when: The scan of the buyer and seller APIs shows no open high-severity finding, and payout bank-detail changes require re-authentication.

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