

Testing checklist: loyalty program app

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

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

☐ 1. release smoke tests

Done when: On every build, a test member signs in, scans a receipt or purchase, sees points arrive and redeems a reward without a crash.

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

☐ 2. end-to-end functional tests

Done when: A member who earned points before a terms change can still redeem them at the old price shown on their statement.

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

☐ 3. penetration testing

Done when: A tester replaying leaked password lists is throttled and blocked, and cannot read or redeem another member's balance by changing an account number.

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

☐ 4. data integrity and migration testing

Done when: After a ledger migration or program merge, every member's points balance and tier on a full export matches the old system at the published conversion ratio.

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

☐ 5. unit tests

Done when: For a fixed set of sample members, redemption prices for points earned before a terms change stay at the old award price, and earn rules for each tier and promotion produce the points listed in the program terms.

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

☐ 6. exploratory testing

Done when: A session log lists attempts at credential stuffing, detaching a linked stored value card, duplicate receipt scans, referral loops and refund-after-redeem, with the outcome of each and a ticket for every success.

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

☐ 7. payment and money-flow testing

Done when: A stored value top-up and spend each show once on the member statement and in the sandbox, and the stored value card cannot be moved to another account without signing in again.

Risks: money-loss. Tool class: API client. Usually run by: QA engineer.

☐ 8. compliance checks

Done when: Each change to earn rates, award prices or expiry is checked against the program terms and notice period before release, and paid point sales follow the store billing rules.

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

☐ 9. integration tests

Done when: After points move to a new ledger or a second program merges in, the balance and tier a member sees in the app, at the point of sale and in a partner channel equal the converted balance in the new ledger, and a new purchase in each channel credits points once.

Risks: data-corruption. Tool class: API client. Usually run by: developer.

☐ 10. security scanning

Done when: The scan report for the member API has no open high findings, and membership numbers never appear in page addresses, emails or support exports.

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

☐ 11. device and browser compatibility

Done when: Sign-in, earn and redeem complete on the oldest supported iOS and Android versions and on the web member area.

Risks: store-rejection. Tool class: device cloud. Usually run by: QA engineer.