

# Testing checklist: email marketing platform

Source: <https://howtotestaproduct.com/how-to-test/email-marketing-platform/>

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

## ☐ 1. release smoke tests

Done when: After every deploy, a test campaign to seed inboxes at Gmail and Yahoo lands in the inbox with SPF, DKIM and DMARC shown as pass in the headers.

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

## ☐ 2. end-to-end functional tests

Done when: A subscriber who joins through double opt-in, receives a campaign and unsubscribes in one click gets no later campaign from any list in that account.

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

## ☐ 3. regression suite

Done when: The unsubscribe, suppression and consent-capture cases rerun on every release, and a single failure blocks it.

Risks: data-corruption, regulatory-penalty. Tool class: test management. Usually run by: QA engineer.

## ☐ 4. data integrity and migration testing

Done when: After a list import or merge, previously suppressed contacts stay suppressed and every imported contact shows a consent source and date.

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

## ☐ 5. unit tests

Done when: The suppression step drops every unsubscribed, bounced and complained address from a fixed send list before the send queue is built.

Risks: regulatory-penalty. Tool class: unit framework. Usually run by: developer.

## ☐ 6. compliance checks

Done when: Every campaign template carries a working unsubscribe link and the sender's postal address, and sending is blocked until both are present.

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

## ☐ 7. integration tests

Done when: Clicking one-click unsubscribe in a Gmail or Yahoo seed inbox removes the contact once, and a link scanner opening the same link leaves the contact shown as subscribed in the audience list.

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

## ☐ 8. security scanning

Done when: The scan report for the app and API has no open high finding that exposes subscriber lists or sending domain settings, and API keys are shown once at creation and masked afterwards.

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

## ☐ 9. penetration testing

Done when: A tester holding a staff support account cannot export a customer's audience or change its sending domain without a logged customer approval.

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