

Testing checklist: ERP system

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

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

☐ 1. release smoke tests

Done when: After every deploy, a test payroll run for a fixed set of employees produces the expected net pay for each person.

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

☐ 2. regression suite

Done when: The payroll, posting and period-close cases rerun on every release, and a single difference in totals blocks it.

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

☐ 3. unit tests

Done when: Each pay rule returns the expected amount for fixed edge cases: mid-period hire, retroactive raise, unpaid leave and termination.

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

☐ 4. end-to-end functional tests

Done when: Procure-to-pay and hire-to-pay scenarios run with real pay rules and real users, and every invoice and payslip matches the expected amount.

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

☐ 5. data integrity and migration testing

Done when: After migration, the trial balance, open payables and employee records match the legacy system to the cent and to the record.

Risks: data-corruption, wrong-decisions. Tool class: data validation. Usually run by: QA engineer.

☐ 6. compliance checks

Done when: An auditor can trace each line of the month-end report to its source postings, and the patch level of every module is recorded against the vendor's advisories.

Risks: wrong-decisions, data-breach. Tool class: test management. Usually run by: product manager.

☐ 7. integration tests

Done when: Every field sent by each feeder system arrives in the ledger posting, and a missing required field rejects the batch with a visible error.

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

☐ 8. security scanning

Done when: The scan report for every internet-facing ERP portal shows no open high findings and the latest vendor security patch applied.

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

☐ 9. penetration testing

Done when: An unauthenticated tester cannot reach any file, report or servlet behind the supplier or employee self-service portal.

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