

# 25 Questions to Ask Before Approving an IT Change

A practical readiness checklist for IT Change Managers, CAB members, technical owners, and approvers.

Strong approvals begin with better questions. Use this checklist before approval, during CAB, or while coaching implementation teams.

## 1 • PURPOSE & SCOPE

1. What business or technical outcome is this IT Change intended to achieve?
2. Is the scope specific, complete, and understandable to someone outside the implementation team?
3. Which systems, services, applications, infrastructure components, or configuration items are affected?
4. Are any related activities, dependencies, or supporting IT Changes missing from the record?
5. Does the planned implementation match the scope described in the IT Change request?

## 2 • RISK & IMPACT

6. What could realistically go wrong during or after implementation?
7. Who or what could be affected - customers, employees, business processes, data, vendors, or downstream services?
8. Is the assigned risk level supported by the actual complexity, impact, timing, and dependencies?
9. Are security, regulatory, financial, data-quality, or operational risks involved?
10. Could this IT Change conflict with another IT Change, release, maintenance event, blackout period, or peak business activity?

## 3 • TESTING & READINESS

11. What testing was completed, and where was it performed?
12. Do the test results demonstrate that the intended outcome was achieved?
13. Were negative scenarios, integrations, dependencies, and potential failure conditions tested?
14. Are required approvals, resources, access, tools, and implementation participants confirmed?
15. Are implementation steps sequenced, detailed, and clear enough for another qualified person to follow?

## 4 • RECOVERY & CONTINUITY

16. What specific conditions will trigger a backout or contingency response?
17. Is the backout plan technically feasible, tested when appropriate, and detailed enough to execute?
18. If backout is not possible, is the reason documented along with a credible contingency or mitigation plan?
19. How long will recovery take, and does that duration fit within the approved window and business tolerance?
20. Are backups, restore points, validation steps, escalation contacts, and decision authority confirmed?

## 5 • COMMUNICATION & VALIDATION

21. Who must be notified before, during, and after the IT Change?
22. Are the implementation window, outage expectations, customer impact, and support needs clearly communicated?
23. What monitoring will identify unexpected behavior during and after implementation?
24. What measurable evidence will confirm that the IT Change was successful?
25. Who owns post-implementation validation, documentation updates, issue follow-up, and closure?

## Final Decision Check

Before approving, can you confidently say:

- ☐ The outcome and scope are clear.
- ☐ The risk and impact are understood.
- ☐ Testing supports implementation readiness.
- ☐ Recovery or contingency is credible.
- ☐ Dependencies and conflicts have been addressed.
- ☐ Communications and resources are confirmed.
- ☐ Success can be measured and ownership is clear.

A strong IT Change process is not about creating more paperwork. It is about making risk visible early enough to act.

For educational and professional-development purposes. Adapt this checklist to your organization's policies, risk appetite, and regulatory requirements.