

User Access & ITGC Checklist

A practical checklist for access provisioning, privileged users, periodic review and change governance.









How to use this checklist

This checklist is designed as a practical fieldwork aid for user access & itgc. Use it to prepare interviews, structure testing and document areas requiring deeper evidence. A checked box should mean the point was considered and supported - not simply that a question was asked.

SIMPLE STATUS KEY

- ☐ **Done** Evidence supports the point
- ☐ **Review** More evidence or clarification needed
- ☐ **N/A** Not applicable - document why

Access lifecycle

- ☐ **01** Access requests specify business need and required role.
- ☐ **02** Manager and system-owner approvals are obtained.
- ☐ **03** Role design follows least privilege.
- ☐ **04** Leaver access is disabled promptly across key systems.
- ☐ **05** Mover access is adjusted instead of simply adding roles.

AUDITOR NOTES / EVIDENCE

Privileged access

- ☐ 06 Admin accounts are limited and separately identified.
- ☐ 07 Privileged activity is logged and reviewed.
- ☐ 08 Shared privileged credentials are avoided or tightly controlled.
- ☐ 09 Emergency access is time-bound and retrospectively reviewed.
- ☐ 10 Service accounts have owners and appropriate credential controls.

Risk prompts

- What could fail even if the documented procedure looks adequate?
- Where can one person initiate, change and approve the same outcome?
- Which exceptions are common enough to have become normal practice?
- What data pattern would indicate control bypass or management override?

TESTING NOTES / EXCEPTIONS

ITGC basics

- ☐ 11 Periodic user-access review is evidence-based.
- ☐ 12 Production changes are approved, tested and segregated.
- ☐ 13 Critical jobs/interfaces are monitored for failures.
- ☐ 14 Backups are tested for restoration where relevant.
- ☐ 15 Security incidents and repeated access exceptions are tracked.

Evidence to retain

- ☐ 01 Relevant system reports or extracts with source and period visible.
- ☐ 02 Approval/workflow evidence for selected high-risk items.
- ☐ 03 Screenshots or logs supporting key control steps and exceptions.
- ☐ 04 Reconciliations or reperformance showing how the conclusion was reached.
- ☐ 05 Management explanation only where corroborated or clearly identified as explanation.

Use data to challenge the checklist

Where transaction data is available, do not rely only on samples. Run targeted tests that identify unusual behavior, control bypass and concentrations. Adapt the tests below to the process and available fields.

- ☐ **01** Trend exceptions by user, approver, location, vendor/customer or month.
- ☐ **02** Identify transactions just below approval or policy thresholds.
- ☐ **03** Search for duplicates, repeated round values and unusual timing.
- ☐ **04** Compare master-data changes with subsequent transactions or payments.
- ☐ **05** Review override, manual-entry and emergency/urgent indicators.
- ☐ **06** Investigate outliers that combine multiple risk indicators.

RED-FLAG RULE

A red flag is not proof of wrongdoing. Treat it as a reason to obtain more evidence. Combine pattern, business context, approval history and supporting records before reaching a conclusion.

Completion and conclusion

Before you close the checklist

- ☐ **01** All material exceptions have an evidence reference.
- ☐ **02** Open questions have an owner and due date.
- ☐ **03** Control design issues are separated from isolated execution errors.
- ☐ **04** Recurring exceptions have been considered for root cause and systemic impact.
- ☐ **05** The conclusion is proportionate to evidence and business risk.
- ☐ **06** Any issue requiring escalation has been communicated promptly.

FINAL CONCLUSION

Overall assessment / key message:

Owner / follow-up date:
