

FREE PRACTICAL GUIDE

INTERNAL AUDIT RESOURCE LIBRARY

IT AUDIT

How to Audit User Access & ITGC Basics

A practical guide to access governance, joiner-mover-leaver controls and privileged activity

Why this guide matters

How to Audit User Access & ITGC Basics

This guide is designed for internal auditors who need a concise, practical way to apply audit user access & itgc basics in real engagements. It focuses on decisions, evidence and common failure points rather than theory.

THE OUTCOME YOU WANT

A practical guide to access governance, joiner-mover-leaver controls and privileged activity.

The six-step approach

- 1 Identify critical systems, roles and privileged functions.
- 2 Review joiner, mover and leaver access workflows.
- 3 Test approvals and timely removal of access.
- 4 Analyze privileged, shared, generic and dormant accounts.
- 5 Review periodic access recertification and evidence of challenge.
- 6 Assess change-management and logging controls that support reliable access governance.

Steps 1-3: Build the foundation

How to Audit User Access & ITGC Basics

1

Identify critical systems, roles and privileged functions.

Define the decision, risk or process question before collecting evidence. Write down what a good outcome would look like.

2

Review joiner, mover and leaver access workflows.

Use actual transactions, system evidence, data and accountable owners to confirm how the process operates in practice.

3

Test approvals and timely removal of access.

Record assumptions, exceptions and boundaries early so later testing remains focused and reproducible.

AUDITOR PROMPT

Ask: "What evidence would convince another experienced auditor that this conclusion is reasonable?" If the answer is unclear, strengthen the planned work before moving on.

Steps 4-6: Turn work into assurance

How to Audit User Access & ITGC Basics

4

Analyze privileged, shared, generic and dormant accounts.

Match the depth of work to the severity of the risk. High-risk conclusions need stronger evidence and clearer documentation.

5

Review periodic access recertification and evidence of challenge.

Challenge exceptions for frequency, impact, root cause and management awareness before deciding what they mean.

6

Assess change-management and logging controls that support reliable access governance

Finish with an explicit conclusion and next action: no issue, improvement opportunity, finding, escalation or follow-up.

QUALITY CHECK

Before you finalize, ask whether the work directly answers the original audit question, whether evidence is sufficient, and whether a reader can understand the reasoning without being in the audit team.

TEST

Compare active ERP users to current employee records and termination dates.

EXCEPTION

Former employee account remains active with purchasing rights.

FOLLOW-UP

Confirm last login, activity, ownership of deprovisioning and whether monitoring detected the issue.

What makes the example useful?

- It starts from a specific risk or audit question.
- It connects evidence and testing to a conclusion.
- It avoids treating process description as proof of control effectiveness.
- It leaves a clear path for management action or follow-up.

Quick reference - use this on your next audit

How to Audit User Access & ITGC Basics

Five practical reminders

- Focus first on access that can create, approve, change or conceal high-risk transactions.
- Terminated-user access and privileged accounts are high-value tests.
- A signed recertification sheet is weak if reviewers cannot understand the entitlements.

Mini self-check

- ☐ Have I linked the work to a clear audit objective or business risk?
- ☐ Is the evidence strong enough for the importance of the conclusion?
- ☐ Have I distinguished facts, explanations and assumptions?
- ☐ Have I considered root cause and recurrence, not only the immediate exception?
- ☐ Can management understand what decision or action is required?

RESOURCE NOTE

This is a practical learning resource, not formal professional guidance. Adapt the approach to your organization, applicable standards, regulation and audit methodology.