Guide

User Access Review Checklist

What to Include + Free Downloadable

Table of Content

What to Include
+ Free Downloadable template

If you're a GRC, security, or compliance leader preparing for a SOC 2, SOX, or ISO 27001 audit, a well-executed User Access Review (UAR) isn't just a checkbox—it's a critical control. But without a reliable process, these reviews can quickly become chaotic, inconsistent, or incomplete.

To make things easier, we've built a **practical, step-by-step checklist and a downloadable template** designed specifically for risk and compliance teams. Whether you're running your first access review or scaling reviews across dozens of systems, this guide helps ensure your process is thorough, repeatable, and audit-ready.

1. Review Setup

Define Scope:
Start by identifying all systems, applications, and teams involved. Missing a critical system can create audit gaps or security blind spots.

Set Frequency:
Set review cadences based on system sensitivity and regulatory requirements. Quarterly reviews are common for high-risk apps; annual may be sufficient for low-risk areas.

Assign Owners:
Designate system owners or managers who have the context to evaluate access. Clear ownership eliminates confusion and speeds up the decision-making process.

Clarify Roles:
Provide clear guidance on what's expected from each reviewer. A simple walkthrough or quick-reference guide can reduce mistakes and ensure consistency.

Confirm Availability:
Check that reviewers are available during the review window. If someone is out, proactively assign a delegate with similar access context and authority.

2. Data Preparation

Sync HRIS:

Pull current employee and contractor data from platforms like Workday or BambooHR. Up-to-date identity data ensures accuracy and completeness and highlights any recent organizational changes. Automated syncs reduce manual errors and saves time.

Pull Identity & Access Data:

Gather user and group access data from identity providers like Okta or Azure AD. This helps reviewers see who has access and to what.

Extract Application Entitlements:

Collect role or permission-level data from each system. Collaborate with application owners to ensure accuracy.

Identify Risky Access:

Highlight dormant accounts, over-provisioned users, and segregation of duties (SoD) issues. These should be top priorities during the review.

Map Access with Context:

Provide business context for each access entry—job function, department, recent activity. The easier it is to assess, the faster and more accurate your reviews will be.

3. Pre-Review Communication

Notify Reviewers:
Send clear, timely notifications (via email, Slack, Teams or other communication platforms) that include the review timeline, expectations, and who to reach out to in case of any questions.

Share Step-by-Step Instructions:
Give reviewers a structured process: how to review, what to look for, and where to log decisions. Include links to relevant policies for added context.

Set Realistic Deadlines:
Define review deadlines and outline escalation paths in case of delays. Clarity around timing increases participation and accountability.

Enable Delegation:
Allow reviewers to assign a delegate when they're unavailable. If using a platform like BalkanID, managers can assign delegates directly within the interface—ensuring reviews stay on track.

4. Review Execution

Approve or Reject Access with Context:

Reviewers assess access against job responsibilities, recent usage, and flagged risks. Justifications should be captured for any sensitive access retained.

Leverage Recommendations:

Leverage automation to handle routine access reviews, but always ensure human oversight on high-risk permissions.

Prioritize High-Risk:

Prioritize administrative access, sensitive data, and SoD violations. These areas carry the greatest audit and security risk.

Capture Reviewer Notes:

Record explanations and reviewer notes to support transparency, justify decisions, and provide context for future audits or reviews.

5. Remediation

Revoke Access:
Use automated workflows or ITSM tools (like Jira or ServiceNow) action on decisions.

Track Completion:
Monitor open items and follow up on delays. Keeping stakeholders informed ensures momentum and accountability.

Reconfirm Actions:
Notify reviewers once their actions have been implemented. This reinforces trust and signals that the feedback loop is closed.

6. Audit & Reporting

Export Reports:
Export review results in CSV or PDF formats. Include who reviewed what, when, and what decision was made.

Ensure Traceability:
All decisions should be time-stamped, attributed, and documented. This is crucial for audits and internal reviews.

Document Exceptions:
Not all access decisions are black and white. Where exceptions exist, ensure they are well-documented with rationale and approvals. This helps auditors understand risk management decisions.

7. Continuous Improvement

Analyze Participation:
Track completion rates and reviewer accuracy. If participation is low or errors are high, target training and support accordingly.

Spot Trends:
Are certain teams consistently over-provisioned? Are dormant accounts common in specific systems? Use the data to drive improvements.

Refine Process:
Adjust review frequency, scope, or team involvement based on the learnings. Iterate to make the process leaner and more effective. Document changes for audit purposes.

Automate Scheduling:
Schedule future access review process automatically using your UAR platform. Automation reduces the risk of human error and ensures consistency at scale.

Free Downloadable Template

User Access Review Checklist

To help you put this into action, we've created a simple, customizable checklist that aligns with the process above. Track owners, deadlines, and completion status all in one place.

Step	Description	Owner	Deadline	Status
Define Scope	Document systems, apps, and departments in scope	GRC Lead	DD/MM	
Assign Reviewers	Identify managers, system/app owners to review relevant access	GRC	DD/MM	
Sync Identity Data	Pull latest user/ contractor info from HRIS and identity providers	IT	DD/MM	
Flag Dormant Users	Inactive > 90 days (or as per Infosec policies)	Security	DD/MM	
Notify Reviewers	Email/Slack reminders	GRC	DD/MM	
Approve/ Reject Access	With proper justification	Reviewer	DD/MM	
Trigger Revocations	Trigger removal workflows (ITSM/De-provisioning etc.)	IT	DD/MM	
Export Reports	Export for audit purposes	Compliance	DD/MM	
Store Artifacts	Secure archive folder	Compliance	DD/MM	
Map User Roles & Access	Document user roles, departments, and current access rights	IT	DD/MM	

Consider These Supporting Questions:

What happens if a reviewer doesn't respond in time?

Who owns resolution for access conflicts or exceptions?

How are vendor and third-party users included in the review?

Running a successful access review doesn't have to be complex or time-consuming. With a structured process and the right tools, you can reduce audit stress, improve security, and build trust with stakeholders.

Download our free checklist template today and bring structure and clarity to your next access review cycle.

Request Demo