Guide

User Access Review for SOC2, HIPAA, and ISO Compliance

Table of Content

In today's regulatory landscape, organizations face increasing pressure to demonstrate that they can securely manage user access to critical systems and sensitive data. For businesses preparing for or undergoing compliance audits, User Access Reviews have become a non-negotiable component of meeting regulatory requirements. Whether you're working toward SOC 2 certification, HIPAA compliance, or ISO 27001 certification, effective access reviews are a cornerstone of your security and compliance strategy. When done right, they provide clear evidence of who has access to what, and why — giving auditors confidence and helping your organization stay secure.

On the other hand, poorly executed or neglected access reviews can lead to failed audits, regulatory penalties, and serious security risks. In fact, recent studies show that 80% of cyberattacks involve identity-based techniques, underscoring the importance of robust access control—not just for compliance, but as a key part of your overall security posture.

This guide provides a clear, step-by-step roadmap for conducting UAR compliance that meets the specific requirements of SOC 2, HIPAA, and ISO 27001 frameworks.

What Are User Access Reviews in the Context of Compliance?

For compliance purposes, UARs go beyond routine IT maintenance tasks. They create documented evidence of access governance, demonstrate control over sensitive information, and provide auditors with clear visibility into how organizations manage user permissions. The review process typically involves identifying all users with system access, documenting their current permissions, evaluating whether access remains appropriate, and taking corrective action when discrepancies are identified.

The core compliance principles that UARs satisfy include establishing least privilege access, where users receive only the minimum permissions required for their job functions. They enforce role-based access control by validating that access aligns with defined organizational roles and responsibilities. UARs also ensure timely access revocation, particularly when employees change roles or leave the organization.

For compliance purposes, UARs go beyond routine IT maintenance tasks. They create documented evidence of access governance, demonstrate control over sensitive information, and provide auditors with clear visibility into how organizations manage user permissions. The review process typically involves identifying all users with system access, documenting their current permissions, evaluating whether access remains appropriate, and taking corrective action when discrepancies are identified.

Why UARs Matter for Compliance

Identity Governance:
UARs are a core pillar of identity governance and access management (IGAM), ensuring that access aligns with business roles and regulatory requirements.

Principle of Least Privilege:
By regularly reviewing access, organizations enforce the principle of least privilege, reducing the risk of over-privileged accounts and insider threats.

Timely Access Revocation:
UARs help identify and remove access for users who have changed roles, left the company, or no longer need certain permissions—closing a major gap exploited in many breaches.

Core Compliance Principles Satisfied by UARs

Least Privilege:
Only necessary access is granted.

Role-Based Access Control (RBAC):
Access is aligned with job functions.

Timely Revocation:
Access is promptly removed when no longer needed.

Without robust UARs, organizations risk audit failures, regulatory penalties, and reputational harm. Let’s break down exactly what each major compliance framework expects.

Why Compliance Frameworks Mandate UARs

SOC 2: Trust Services Criteria (TSC)

Principles Covered:

Security, Availability, Confidentiality

Requirement:

Organizations must perform periodic access reviews to ensure that only authorized users have access to sensitive systems and data.

Auditor Expectations:

Evidence of reviews, timestamps, approval/revocation decisions, and a clear audit trail.

Common Pitfalls:

Incomplete documentation, lack of review frequency, missing approval trails.

HIPAA: Healthcare Security Rule

Mandate:
Administrative safeguards require regular review of workforce access to electronic protected health information (ePHI).

Focus:
Ensuring only authorized staff can access PHI, and that ex-employees or role changers are promptly removed.

Auditor Expectations:
Documented access review schedules, evidence of access revocation, and justification for all access rights.

Common Pitfalls:
Dormant accounts, over-privileged users, lack of documentation.

ISO/IEC 27001

Best Practices:

Documented reviews, segregation of duties, and clear ownership of the review process.

Auditor Expectations:

Scheduled reviews, evidence of corrective actions, and policy enforcement.

Common Pitfalls:

Ad-hoc reviews, lack of ownership, rubber-stamping approvals.

Compliance-Focused UAR Checklist

A well-structured User Access Review process is your best defense against audit surprises. Use this checklist to ensure you're covering every compliance requirement for SOC2, HIPAA, and ISO 27001.

Step	Requirement	Framework(s) Covered
Define Review Scope	Identify all apps, systems, and data to include	All
Assign Review Owners	Designate managers or app owners for each system	SOC2, ISO
Set Review Frequency	Establish review cadence (quarterly, risk-based, or per policy)	ISO, HIPAA
Collect Access Logs	Gather user access data from IDP, SaaS apps, HRIS	All
Flag Dormant Accounts	Identify accounts inactive for >90 days	HIPAA, SOC2
Review Privileged Access	Pay special attention to admin/service accounts	All
Record Decisions	Document approve/remove actions with reasons	SOC2, ISO
Store Audit Trails	Keep timestamps, reviewer comments, and evidence	All
Remediate Issues	Remove unnecessary access, escalate exceptions	All
Report & Certify	Generate reports for auditors, certify completion	All

Pro Tip:
Download a compliance-ready checklist for your next audit.

How to Automate and Streamline UAR Compliance

Manual UARs—think spreadsheets, emails, and frantic last-minute data pulls—are a recipe for audit anxiety and human error. As organizations scale, the complexity and frequency of reviews multiply, making manual processes unsustainable.

Limitations of Manual UARs

Time-consuming:
Gathering access data from multiple sources is slow and error-prone.

Audit Gaps:
Missing documentation or incomplete trails lead to failed audits.

Reviewer Fatigue:
Manual reviews often result in “rubber-stamping” approvals.

Delayed Remediation:
Revoking access via email or ticketing is inefficient.

Benefits of UAR Automation Tools

System-Generated Recommendations:
Intelligent suggestions to flag risky or unnecessary access.

Reviewer Reminders:
Automated notifications keep reviews on schedule.

ITSM Integration:
Seamless revocation of access via ServiceNow, Jira, etc.

Audit-Ready Reports:
One-click evidence for SOC2, HIPAA, and ISO audits.

What to Look for in a UAR Automation Platform

Comprehensive Coverage:
Integrates with your identity provider, SaaS, and on-prem systems.

Contextual Reviews:
Surfaces user context, role changes, and risk factors.

Continuous Monitoring:
Enables ongoing, not just periodic, access reviews.

Audit Trail:
Stores every decision, timestamp, and comment for easy retrieval.

How BalkanID Helps:

Platforms like BalkanID automate the entire UAR process—making reviews continuous, contextual, and always audit-ready. With built-in compliance mappings, you can pass your next SOC2, HIPAA, or ISO audit with confidence.

See how BalkanID can help you for your next compliance audit.

Best Practices for Maintaining UAR Compliance

Create a Formal UAR Policy:
Document the process, frequency, and responsibilities.

Schedule Regular Reviews:
Monthly or quarterly, based on risk and compliance needs.

Integrate with Joiner-Mover-Leaver Workflows:
Ensure access is reviewed at every stage of the employee lifecycle.

Enforce Reviewer Accountability:
Use dashboards and notifications to track completion.

Run Dry Runs Before Audits:
Simulate reviews to catch gaps before auditors do.

Involve Internal Audit:
Don’t leave reviews to IT alone—engage risk and compliance teams for oversight.

Monitor for Rubber-Stamping:
Analyze approval patterns to detect and address superficial reviews.

Key Takeaways

UARs are Essential:
User Access Reviews are a non-negotiable requirement for SOC2, HIPAA, and ISO 27001 compliance.

Manual Reviews Are Risky:
Spreadsheets and emails can't keep up with modern access complexity or audit scrutiny.

Automation is the Future:
Tools like BalkanID improve accuracy, reduce fatigue, and generate audit-ready evidence.

Use the Checklist:
Whether you're just starting or looking to mature your program, a structured checklist is your best friend for audit readiness.

Ready to take the next step?

Download the compliance ready checklist for your next audit—covering SOC2, HIPAA, and ISO 27001 access review requirements.

Download the UAR Compliance Checklist

Stay ahead of your next audit. Make UAR compliance simple, efficient, and bulletproof.