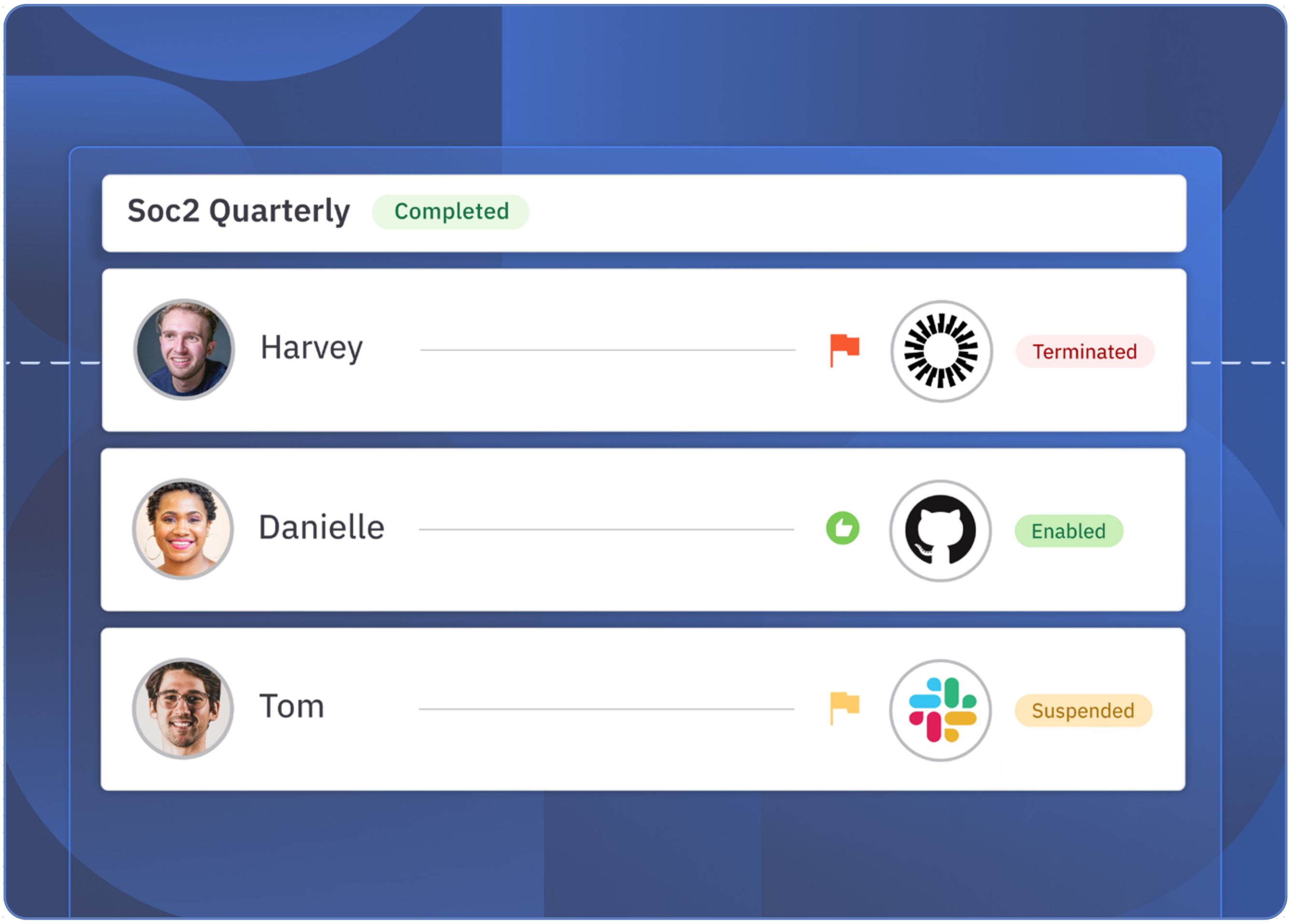
ConductorOne

User Access Reviews: Process & Best Practices Checklist



User Access Reviews are essential for identifying and managing who has access to your organization's critical systems and data. They help ensure that only the right people have access at the right times, reducing the risk of internal data breaches.

Picture this — It's early December 2020, and Nickolas Sharp has just pulled off a cyber-heist on his former employer, a New York–based technology company.

Sharp accessed the company's AWS and GitHub servers unauthorized, stealing gigabytes of sensitive data.

The result?

- $2 million lost to extortion for the return of the files.
- Bad publicity on the company's security integrity.
- Loss of billions of dollars in market value [*]

This situation is far from unique. Insider threats are a concern for 71% of businesses, with 34% reporting that such breaches involved users with high-level access privileges [*].

Now, you may be wondering: *How can organizations (like yours) protect themselves from similar cybersecurity threats?*

The answer lies in a critical best practice: User Access Reviews

What Is a User Access Review?

A User Access Review (UAR) is a critical process that involves examining and validating user access rights within an organization's systems and applications.

This process ensures the right individuals have appropriate access levels based on their job roles and responsibilities.

Take this for example —

A scenario in a healthcare setting where a nurse leaves the job but still retains access to patient records. Without a regular user access review, this access could remain unnoticed, posing a significant privacy and security risk. A UAR process would identify this unnecessary access right, ensuring it's revoked promptly to protect patient confidentiality and comply with healthcare regulations.

Who Is Considered a "User" in User Access Reviews?

In the context of User Access Reviews, **a "user" is any individual who has access to an organization's systems, applications, or data.**

This can include a wide range of roles, such as:

- **Employees.** Full-time, part-time, or temporary staff who need access to company resources to perform their job functions.
- **Contractors.** External individuals or entities engaged by the organization for a specific task or project who require access to certain systems or information.
- **Consultants.** External advisors or experts who are given access to specific parts of the organization's IT environment to provide their services.
- **Partners.** Business partners who may need access to certain systems or data as part of a collaborative relationship with the organization.

💡 **Fully automated user access reviews:**

Maintain compliance, reduce standing privileges, and improve security without manual effort.
Explore ConductorOne's Access Reviews Product

Why Are User Access Reviews Important?

1. Helps Prevent Unauthorized Access

Over time, employees' roles and responsibilities change, leading to individuals retaining access rights that are no longer necessary for their current positions.

UARs help in identifying such discrepancies and revoking access that is no longer needed, thus minimizing the "attack surface" that could be exploited by malicious actors.

This is possible by preventing unauthorized access, particularly insider threats.

While insider threats can manifest in various forms, they're mainly categorized into three main forms: privilege creep, privilege misuse, and privilege abuse.

Privilege Creep This refers to the gradual accumulation of access rights beyond what an individual needs to perform their job functions. This typically occurs over time as employees transition through different roles within the organization, accumulating access rights without having the old ones revoked.

Privilege Abuse This represents a more severe threat, where individuals intentionally exploit their legitimate access for unauthorized or malicious purposes. This could range from data theft and sabotage of IT systems to fraud.

💡 **Real Life Implication:**

We witnessed this happen to Tesla in the summer of 2023 when two former employees leaked the PII of current and former employees of the company to a foreign media outlet [*]

Privilege Misuse This occurs when legitimate access rights are used inappropriately without malicious intent. This could involve accessing data or systems for unauthorized purposes, such as curiosity or convenience, which can lead to compliance violations or unintentional data leaks.

💡 **Real Life Implication:**

A Boeing employee “ignorantly” emailed a spreadsheet containing the personal information of 36,000 of his coworkers to his wife. This cost the company $7 million in payments [*]

2. Helps Meet Compliance Requirements

Strict regulatory standards govern many industries—think Europe’s GDPR for data protection, HIPAA for healthcare, or SOX for financial reporting.

These regulations often mandate regular user access reviews to protect sensitive data from misuse or unauthorized access.

By conducting user access reviews, you have a well-documented history of who has access to what and when changes were made. This documentation is crucial during audits to demonstrate compliance with access control requirements.

Failing to do this can result in violations of regulatory standards, leading to significant fines, legal consequences, and reputational damage.

💡 **Real Life Implication:**

In November 2022, Meta was fined $277 million (€265 million) by the Ireland Data Protection Commission (DPC) for compromising the personal information of 500 million users [*]

3. Helps Reduce Licensing Cost

Many platforms and software applications are priced based on the number of users or the level of access granted to users.

Meaning — the more users, the higher the application cost.

Meanwhile, by clearly understanding the actual software usage and needs through user access reviews, organizations can negotiate more effectively with software vendors. This includes adjusting license quantities, negotiating terms that fit actual usage patterns, and potentially lowering costs by leveraging accurate usage data.

Additional Benefits:

- **Optimization of License Utilization.** Regular reviews allow companies to adjust licenses according to usage, preventing the common issue of paying for unused or surplus licenses. This directly translates to cost savings and more efficient budget allocation.
- **Prevention of Unauthorized Use.** By identifying and mitigating unauthorized software use, also known as "Shadow IT," organizations can avoid the hidden costs and security risks associated with unapproved applications. This control helps in maintaining compliance and avoiding potential legal and financial penalties.
- **Support for Software Asset Management.** Integrating user access reviews into Software Asset Management (SAM) practices enhances the organization's ability to manage software assets effectively. This approach aids in uncovering inefficiencies and reallocating resources to where they are most needed, ensuring that software investments deliver maximum value.

What Are the Regulations and Standards That Require User Access Reviews?

Several international and industry-specific regulations and standards emphasize the importance of conducting regular User Access Reviews.

Here are a few key examples:

General Data Protection Regulation (GDPR)

Scope: Applies to all organizations processing the personal data of individuals in the EU, regardless of the organization's location.

Requirements for UARs:

- Organizations must implement appropriate technical and organizational measures to ensure and demonstrate that data processing is performed in accordance with GDPR (Article 24 — 43 controller and processor).
- Access to personal data must be limited to authorized personnel whose job roles require access (Principle of Least Privilege).
- Regular review and access rights updates are necessary to ensure ongoing compliance with GDPR's data protection principles.

Health Insurance Portability and Accountability Act (HIPAA)

Scope: Applies to covered entities and business associates in the healthcare sector in the United States.

Requirements for UARs:

- The Security Rule mandates the implementation of technical policies and procedures for electronic information systems that maintain electronic protected health information (ePHI) to allow access only to those persons or software programs that have been granted access rights (§164.312(a)(1)).
- Regular audits and reviews of access records ensure compliance with the Privacy Rule, which protects individuals' medical records and other personal health information.

💡 **Electronic Protected Health Information (ePHI):**

This refers to any protected health information (PHI) that is created, stored, transmitted, or received in any electronic form or media relating to:

- The individual's past, present, or future physical or mental health or condition.
- The provision of healthcare to the individual.
- The past, present, or future payment for providing healthcare to the individual.

Recommended → Learn about Health Information Trust Alliance (HITRUST)

Sarbanes-Oxley Act (SOX)

Scope: Applies to all public companies in the United States and international companies with registered equity or debt securities with the Securities and Exchange Commission (SEC).

Requirements for UARs:

- SOX requires establishing internal controls and procedures for financial reporting to reduce the risk of fraud.
- Section 404 mandates that management and auditors establish and verify controls over access to financial systems and data privacy.
- Regular UARs ensure that only authorized individuals can access financial information, supporting the integrity of financial reporting.

Recommended → What is the Difference Between SOX and SOC Compliance?

ISO/IEC 27001

Scope: International standard that specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS).

Requirements for UARs:

- Clause 9.2 requires regular audits to assess whether the organization's access control policy is followed, including reviewing user access rights at regular intervals.
- The standard emphasizes the importance of managing access to sensitive information and systems and ensuring access rights are granted according to the least privilege principle.

Payment Card Industry Data Security Standard (PCI DSS)

Scope: Applies to all entities that store, process, or transmit cardholder data.

Requirements for UARs:

- Requirement 7 mandates that access to cardholder data and systems should be restricted to only those individuals whose job requires such access.
- Requirement 8.1.6 requires the review of user access rights at least every six months.
- UARs are critical for ensuring that only authorized personnel can access cardholder data, reducing the risk of unauthorized access and data breaches.

These regulations and standards highlight the critical nature of managing access rights effectively to protect sensitive information and ensure compliance.

Organizations of all kinds are subject to these regulations and must establish and maintain processes for regular User Access Reviews. This ensures that access is granted based on necessity and is regularly evaluated to address any changes in job roles, employment status, or risk profile.

Here’s the 5 Step User Access Review Process

Step 1: Create a Framework for the Review

Objective: To establish a clear structure for the entire user access audit process, including scope, timeline, and stakeholders involved.

Define the Scope

- Begin with a comprehensive inventory of all systems, applications, and data repositories. This inventory should include on-premises and cloud-based assets, ensuring nothing is overlooked.
- Prioritize systems and data based on their sensitivity and the potential impact on the organization if compromised. High-risk areas, such as financial systems, HR databases, and customer data repositories, should be at the forefront of the UAR.
- Identify all regulatory requirements affecting your organization. For instance, if you’re subject to GDPR, any system processing the personal data of EU citizens must be included. Similarly, healthcare organizations must prioritize systems containing PHI under HIPAA regulations.
- Don’t overlook third-party and vendor access. Any external system or service with access to your network should also be included in the UAR scope.

Set the Objectives

- **Compliance Objectives.** Clearly define the compliance standards the review is aiming to meet. This could include industry-specific regulations, such as HIPAA for healthcare or PCI DSS for payment card information and general data protection laws like GDPR.
- **Security Objectives.** Define security goals such as minimizing the risk of data breaches, ensuring the principle of least privilege, and maintaining confidentiality, integrity, and data availability. You can also tailor objectives to organizational risk tolerance and security posture, focusing on critical assets and potential threat vectors.
- **Operational Objectives.** Lastly, set objectives around streamlining access to ensure employees have only the access they need, reducing administrative overhead and improving system performance. This could include identifying redundant and outdated access rights reducing the risk of privilege misuse.

Identify All Necessary Stakeholders

- Compile a list of internal stakeholders involved in the UAR process. This typically includes IT security teams, department heads, system owners, and HR for insights into role changes and terminations.
- Determine if external auditors or consultants will be involved in the review process, especially for organizations under stringent regulatory scrutiny. Their expertise can offer an unbiased view and help ensure compliance.
- Establish clear communication channels and responsibilities among stakeholders to facilitate information sharing and decision-making throughout the UAR process.

Schedule the Review

- Develop a realistic timeline for the user access review, considering the availability of stakeholders, the complexity of systems involved, and any external factors such as regulatory deadlines.
- Set specific milestones and checkpoints throughout the review timeline. This allows for progress monitoring and ensures the review stays on track.

Recommended → 7 Principles for Least Privilege Access Implementation

Step 2: Identify and Collect Access Data from Systems and Applications

Objective: To compile an exhaustive list of all assets within the organization, including hardware and software. This should cover servers, workstations, network devices, cloud services, databases, and other repositories where sensitive data might be stored or processed.

Pro Tip

For each identified system, understand the mechanism for logging and reporting access data.

Extract the Data

You can choose to automate this process or do it manually (or both).

- **Using Automated Tools/Scripts.** Extract access data from systems whenever possible. This reduces manual effort and the potential for errors. Ensure the data extraction methods capture all necessary details, such as user names, roles, access levels, and last access timestamps.
- **Using Manual Processes.** In cases where automated tools cannot be used—perhaps due to system compatibility issues or the absence of such tools—manual processes must be employed. This involves system administrators manually compiling access rights lists from each system and application.

Pro Tip

Ensure the extraction process covers every piece of data relevant to access control, including but not limited to user accounts (employee ID, username), group memberships, specific permissions (read, write, execute), and any special access rights.

Centralize the Data

- Consolidate the extracted data into a centralized database or access management tool. This could be a specialized identity governance platform, a secure database, or even a managed spreadsheet, depending on the complexity and size of your organization.
- Categorize assets based on their function, data sensitivity, and user base. For instance, categorize them into critical systems, internal applications, third-party services, etc.
- Organize the data to allow for efficient sorting, filtering, and querying. For instance, data can be categorized by department, role, system/application, or access level. This organization is crucial for the subsequent steps of the UAR process, enabling quick identification of potential access issues.
- Ensure the database or tool where access data is stored is secure and accessible only to authorized personnel involved in the UAR process. The integrity and confidentiality of this data are crucial, as it contains sensitive information about organizational access.

💡 **Pro Tip**

Map data flow to understand how data moves between systems. This can help identify indirect access requirements or dependencies that might not be immediately apparent.

Validate the Data

- **Cross-Reference with HR Records.** Validate the collected access data against HR records to verify its accuracy. This step is essential for identifying discrepancies such as access rights assigned to employees who have left the organization, transferred departments, or changed roles.
- **Identify Inactive Accounts.** Look for accounts that have not been used for an extended period, as these are often overlooked sources of potential security risks. Inactive accounts should be flagged for further review and potentially deactivated.
- **Reconcile Accounts.** Reconcile any discrepancies found during the validation process. This might involve updating access rights to reflect recent hires, role changes, or terminations and removing access from accounts that are no longer active or relevant.
- **Document the Process for Auditing.** Document the validation process, including any discrepancies identified and the steps to reconcile them. This documentation will be crucial for audit purposes and tracking changes over time.

💡 **Pro Tip**

Leverage identity and access management (IAM) tools, asset management software, and data classification tools to automate parts of the scope definition process.

Step 3: Review and Verify All Access Rights

Objective: To assess whether the current access rights are appropriate based on job roles and responsibilities.

Employ Role-Based Access Control (RBAC) and Verification

Role-Based Access Control (RBAC) is an approach that simplifies access management by assigning rights and permissions to roles rather than to individual users.

It operates on the principle that access to resources should be based on the roles within an organization, reflecting the specific job functions.

A role defines a set of permissions required to perform a job. Users are then assigned to these roles, inheriting the permissions associated with them.

To do this:

- Begin by mapping each user's access rights to their specific job functions. This involves a detailed review of job descriptions, roles, and responsibilities to understand what access is necessary for each position.

💡 **Pro Tip**

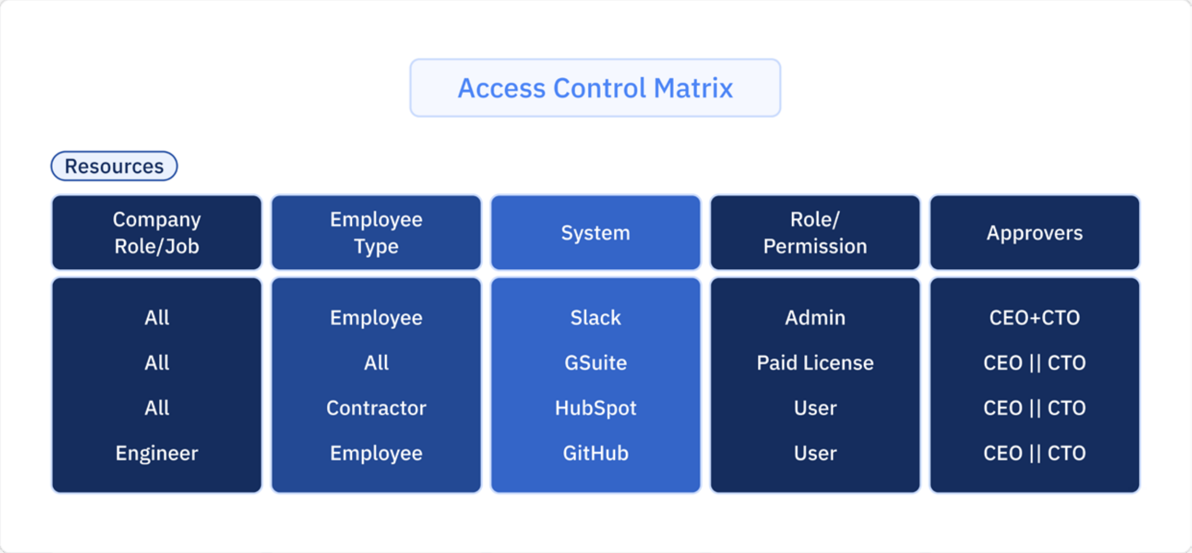
Work closely with department heads and managers to gain insights into the unique requirements of each role. This collaboration is crucial for accurately determining the necessity of access rights, as they have the best understanding of their team's operational needs.

Utilize Access Control Matrix (ACM)

An Access Control Matrix is a table that maps users (or subjects) against resources (or objects) to specify the access rights each user has over each resource.

In simpler terms — the access control matrix serves as a model to describe the rights of each user regarding access to various resources within a system.

The rows of the matrix represent users, and the columns represent resources. Each cell in the matrix specifies the type of access rights (such as read, write, execute, delete) a user has over a resource.



Access Control Matrix

Resources

Company Role/Job	Employee Type	System	Role/ Permission	Approvers
All	Employee	Slack	Admin	CEO+CTO
All	All	GSuite	Paid License	CEO || CTO
All	Contractor	HubSpot	User	CEO || CTO
Engineer	Employee	GitHub	User	CEO || CTO

This matrix is particularly important in ensuring that users have the appropriate levels of access to perform their job functions while preventing unauthorized access to sensitive information.

Implement the Principle of Least Privilege (PoLP)

This dictates that users, systems, applications, and processes should be granted the minimum levels of access—or the "least amount of privilege"—necessary to perform their functions.

Practical Application:

- **User Accounts.** Regular users are provided with standard access rights sufficient for their job functions, while administrative privileges are restricted to those who need them to manage resources.
- **Applications and Systems.** Applications and system processes are given only the permissions necessary to perform their expected duties, limiting their ability to access other parts of the system or network.
- **Temporary Privileges.** When higher access levels are temporarily required, systems are in place to grant these privileges on an "as-needed" basis, with automatic revocation after the task is completed.

To do this:

- **Identify Excess Privileges.** Scrutinize the collected access data to identify instances where users have more privileges than their roles require. This could include access to sensitive data, administrative privileges, or permissions to critical systems irrelevant to their current job functions.
- **Prioritize Access Reduction.** For any identified excess privileges, prioritize their reduction or revocation. This step might involve downgrading user roles, removing users from certain groups, or adjusting permissions to align with the least privilege principle.

Run Cross-Departmental Checks

- Establish a process for regular communication between departments to discuss and validate access needs. This is particularly important for roles that involve cross-departmental projects or responsibilities.
- Pay special attention to individuals with cross-functional roles or those involved in multiple projects across different departments. Their access needs may be more complex and require careful consideration to ensure they have the necessary permissions without exceeding the bounds of the least privilege principle.
- Document the rationale for granting specific access rights, especially for complex or cross-functional roles, and obtain approval from relevant department heads. This ensures transparency and accountability in the decision-making process.

Step 4: Identify and Rectify Unauthorized or Inappropriate Access

Objective: To take corrective action to address any identified discrepancies or unauthorized access instances.

Revoke Access Once Detected

- Develop a systematic approach for revoking unauthorized, outdated, or unnecessary access. This plan should prioritize actions based on the risk associated with the access rights in question.
- Work closely with the IT security team to ensure revocations are implemented effectively without disrupting legitimate business processes. This might involve scheduling changes during off-peak hours or providing temporary access under supervision if immediate revocation could impact critical operations.
- Establish a protocol for notifying affected users and their managers about the revocation of access rights. Communication should explain the reasons for the revocation and, if applicable, the *process for requesting reinstatement of access under the proper protocols.

Adjust All Roles Accordingly

- Once unauthorized access is identified and revoked, assess the current roles of affected users to determine if adjustments are necessary. This could involve redefining job responsibilities, adjusting roles within systems, or changing group memberships to better align with actual job functions.
- Implement role adjustments in a controlled manner, ensuring that users receive only the access rights necessary for their roles. This may require creating new roles or permissions sets more accurately reflecting job responsibilities.
- After adjustments are made, solicit feedback from users and their managers to ensure that the changes have not impeded their ability to perform job functions. Be prepared to make further adjustments as necessary based on this feedback.

Step 5: Document the Review Process and Findings

Objective: To create a comprehensive record of the review process, findings, and corrective actions taken.

Report Every Detail of the Review Process

- Create a detailed report that covers the entire user access review process. This report should include an overview of the review's scope, the methodologies for collecting and analyzing data, a summary of the findings, and a detailed account of the corrective actions undertaken.
- The report should detail specific instances of unauthorized or inappropriate access identified during the review, the rationale behind each decision regarding access revocation or adjustment, and any challenges encountered during the process.

Create an Action Plan

- Based on the review's findings, the report should outline recommendations for enhancing the organization's access control policies, procedures, and practices. This could include suggestions for new tools or technologies to streamline future reviews, employee training on security best practices, or changes to the onboarding/offboarding process to prevent unauthorized access.
- Document all instances of unauthorized or inappropriate access discovered during the review, including details about;
  - the nature of the discrepancy,
  - how it was identified,
  - and the corrective actions taken.
- Also, clearly outline any necessary follow-up actions, assigning responsibility for these actions to specific individuals or departments. This action plan should include deadlines for completion and metrics for evaluating the effectiveness of these actions.

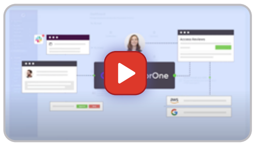
Communicate with Appropriate Stakeholders

- Distribute the report to all key stakeholders, including management, IT security teams, department heads, and any external auditors or consultants involved in the review process. This ensures that everyone involved knows the findings and understands the importance of the actions taken.
- Encourage stakeholders to provide feedback on the report and the review process itself. This feedback can be invaluable for improving future user access reviews.

Create Compliance Documents

For compliance and audit purposes,

- Store the report and all related documentation in a secure, accessible location. This documentation serves as evidence of the organization’s commitment to maintaining robust access control practices and compliance with relevant regulatory requirements.
- Ensure that the documentation is organized to facilitate easy retrieval for audit purposes. This includes the final report and any supporting documentation, such as correspondence with stakeholders, records of meetings, and detailed logs of all actions taken.



How to Run User Access Reviews For Any Application

Watch video here

Best Practices for User Access Reviews [+Checklist]

1. Establishing System Inventories and Identifying System Ownership

System Inventory

You must work with internal security and external auditing teams to gain alignment on this.

This collaboration is crucial for aligning with regulatory compliance frameworks such as SOX, PCI, and SOC2, especially for systems that manage sensitive customer data, financial records, production infrastructure, identity information, or other critical business operations.

Inventory Owners

Once you’ve defined which systems are in scope, identify the application or system owner for each.

For modern enterprises, these systems are increasingly administered outside of IT. While IT may oversee aspects like system availability, procurement, authentication, and single sign-on (SSO) configurations, the ownership of user lifecycle management, permission allocation, and access role definitions frequently reside with different departments.

For example, R&D teams might manage source code repositories, sales operations could oversee customer relationship management (CRM) systems, and human resources might be in charge of the HR information system (HRIS).

2. Implementing Reviews Based on Timing and Frequency

Determine the Frequency

- Start with a comprehensive risk assessment to understand the sensitivity of your organization’s data and systems. Higher-risk areas may require more frequent reviews.
- Consult the specific compliance standards applicable to your organization (e.g., GDPR, HIPAA, SOX) to determine any mandated frequency for access reviews.

- Look to industry benchmarks and best practices as a guide. A semi-annual or annual review cycle is common for many organizations, but this can vary significantly based on the factors above.
- Develop a UAR calendar that outlines when each system, application, or data set will be reviewed over the course of the year.
- Automate Scheduling: Where possible, use governance, risk management, and compliance (GRC) tools to automate reminders and scheduling of UARs to ensure they occur as planned.

Identify Trigger Events

- Significant changes to system infrastructure can alter access needs or introduce new vulnerabilities.
- Promotions, transfers, or departures of employees can significantly affect access requirements.
- Any breach or suspicious activity might necessitate an immediate review of access rights to prevent further unauthorized access.

A good practice is to have a designated team ready to conduct an expedited UAR in response to trigger events. This team should have predefined roles and responsibilities. In addition, integrate UAR triggers into your IT or security incident response platforms to automatically initiate a review process when certain conditions are met.

Other best timing practices include:

- Scheduling UARs at times that align with your organization’s operational calendar. For many, this means conducting reviews after major business cycles, such as the end of the financial year, when systems are less likely to undergo significant changes and staff are more available.
- Identify periods of high activity for your organization, such as end-of-quarter sales pushes or holiday seasons, and plan UARs to avoid these times to minimize disruption.

3. Automating the Review Process

Use Automation Tools and Software

Ideally, you should opt for automation tools and software that automates the collection of user access data and the review process.

This should also include tools that integrate well with the organization’s existing infrastructure (e.g., HR systems, Active Directory/LDAP, cloud services) to automatically update user roles and permissions based on HR events such as hiring, promotion, or termination.

Ensure these platforms offer comprehensive features for managing the entire user access lifecycle, from initiation to review, modification, and documentation. Also, the tool should be able to scale with your organization’s growth and handle the increasing complexity of user access rights over time.

Key Features to Consider When Picking a User Access Review Platform

- Ability to generate tailored reports that meet the specific needs of different stakeholders, including IT, security, compliance, and executive teams.
- Trend analysis for identifying patterns in user access, potential security risks, or compliance issues over time.
- Comprehensive logging and documentation features that provide a detailed audit trail of all UAR activities, changes made, and the rationale behind those changes.

4. Defining the Review Policy

Decentralize Decision-Making

The typical decision-making approach that relies on direct managers for user access reviews is becoming outdated. Companies increasingly recognize the value of engaging app owners, resource owners, or entitlement owners in the review process.

This approach leverages these individuals' in-depth knowledge about their respective areas, enabling more informed decisions regarding user access.

Incorporate Self-Reviews

A good practice in streamlining the review process is the introduction of self-reviews for certain types of access.

This involves users assessing their own need for specific accesses, determining whether it remains critical for their current roles or if they actively use it.

While this method requires subsequent verification from a security perspective, it significantly reduces the workload for app and resource owners and enhances the overall efficiency and effectiveness of access reviews.

Structure the Review Process

For the GRC (Governance, Risk Management, and Compliance) and security teams, identifying a clear plan for reviewing each in-scope system and entitlement is crucial.

This plan should cover several key aspects:

- **Identifying Reviewers.** Determine who will conduct the reviews and the sequence of these reviews. This helps ensure that the review process is both systematic and comprehensive.
- **Fallback Reviewers.** In cases where direct managers or primary reviewers are not identifiable, establish a protocol for who will take on the review responsibility. This ensures that no user access goes unchecked.
- **Requirement for Justification.** Decide whether the user or reviewer must justify ongoing access. This adds an additional layer of scrutiny and accountability to the process.
- **Delegation of Reviews.** Establish rules around whether (and how) reviewers can delegate the review task to someone else. This flexibility can help maintain the review process's flow without compromising security or compliance standards.

Generally, these rules can be pre-packaged into common policies for access reviews and applied across the various systems.

5. Involving the Right Stakeholders in the Review Process

Cross-Functional Teams

Include representatives from IT, security, HR, legal, and relevant business units to ensure all aspects of user access are considered.

IT and security teams bring technical expertise and an understanding of the risks associated with access rights. HR can provide insights into changes in employment status that might affect access needs, while legal teams ensure compliance with relevant laws and regulations.

Department Heads

Engage department heads or managers to validate the necessity of specific access rights for their team members.

These individuals deeply understand the day-to-day operations and can accurately determine the access each employee needs to perform their job functions effectively. Their involvement ensures that the principle of least privilege is maintained, reducing the risk of excessive access that could lead to security breaches.

External Auditors

In cases of compliance audits, involve external auditors early in the process to align on expectations and ensure that the review meets regulatory standards.

Early involvement of auditors can also streamline the review process by identifying potential compliance issues early, allowing for adjustments before formal audits occur.

Listen → A Deep Dive into Compliance with Chris Niggel

6. Ensuring Accuracy and Completeness in the Review Process

Have a Comprehensive User List

This should include everyone with access to the organization’s systems, including contractors, temporary workers, and third-party vendors.

Have Detailed Access Rights

The next step involves compiling a detailed inventory of access rights for each user. This inventory should categorize access rights by system, application, and the data sensitivity level each user can access.

Employ Different Validation Techniques

To validate the accuracy of the information gathered and the decisions made during the review process, employ techniques such as sampling or spot-checking to verify the data’s integrity.

Sampling involves reviewing a subset of users or access rights to infer the accuracy of the entire dataset.

Spot-checking, on the other hand, targets specific, high-risk areas or anomalies for closer examination. These techniques help identify and correct errors in the data, ensuring that the review process is based on accurate and complete information.

7. Training and Awareness for Reviewers

Regularly Train All Reviewers

Provide ongoing training for all individuals involved in the user access review process to keep them updated on the latest security policies, regulatory requirements, and best practices.

This training should ensure all participants in the UAR process are aware of the latest developments in security and compliance. It should also cover a broad range of topics, including the rationale behind UARs, the specifics of the organization’s policies and procedures, and the technical aspects of managing access rights.

Offer Role-Specific Guidance

This training ensures that each participant understands their responsibilities, the scope of their decision-making authority, and the criteria they should use when evaluating access rights.

For example, IT staff may require detailed technical training on the systems and tools used in the UAR process. At the same time, department managers may need guidance on assessing the appropriateness of access levels for their team members.

Conduct Awareness Campaigns

These campaigns highlight the importance of user access reviews in maintaining organizational security and compliance. Organizations can foster a culture of security awareness by raising awareness about the risks associated with improper access rights and the role that UARs play in mitigating these risks. Such campaigns can take various forms, from internal communications and presentations to interactive training sessions and quizzes.

Common Challenges of User Access Reviews

Resource-Intensive and Time-Consuming Process

The entire user access review process demands significant time and resource investment. For starters, the process begins with collecting and aggregating detailed access data from various systems and applications, each potentially having its own set of tools and interfaces for managing user access.

Another overlooked aspect is that it requires a deep understanding of the operational needs of the organization and the potential security implications of each access right. The analyst in charge must painstakingly verify that each user’s access is necessary and appropriate.

Solution:

- Leverage automation and access management tools to streamline user access review processes.
- Implement software solutions for automated data collection, analysis, and reporting.
- Use tools for real-time visibility into user permissions across systems and applications.
- Adopt a role-based access control (RBAC) model to simplify user permissions management.
- Align access rights with job roles to reduce complexity in the UAR process.

Resource-Intensive and Time-Consuming Process

The entire user access review process demands significant time and resource investment. For starters, the process begins with collecting and aggregating detailed access data from various systems and applications, each potentially having its own set of tools and interfaces for managing user access.

Another overlooked aspect is that it requires a deep understanding of the operational needs of the organization and the potential security implications of each access right. The analyst in charge must painstakingly verify that each user's access is necessary and appropriate.

Solution:

- Leverage automation and access management tools to streamline user access review processes.
- Implement software solutions for automated data collection, analysis, and reporting.
- Use tools for real-time visibility into user permissions across systems and applications.
- Adopt a role-based access control (RBAC) model to simplify user permissions management.
- Align access rights with job roles to reduce complexity in the UAR process.

Complex IT Infrastructure

A typical organization runs on a mix of cloud-based services, on-premise systems, and third-party applications. This setup poses significant challenges in maintaining a unified view of user access and permissions, complicating user access reviews.

This is because each platform has its own unique management interfaces and security protocols, adding layers of complexity. Furthermore, custom-built applications or services tailored to specific organizational needs require specialized knowledge for effective access management.

Solution:

- Implement a centralized access management platform that integrates with on-premise, cloud-based, and third-party systems, providing a unified view of all user access rights.
- Deploy IAM solutions with automation features for managing user identities and permissions across diverse environments.
- Use Security Information and Event Management (SIEM) tools to gain insights into access patterns and detect anomalies.

Lack of Visibility into User Permissions Across Systems

The challenge stems from the disparate nature of systems and applications, many of which were not designed to work together or share information seamlessly. This fragmentation hinders the aggregation of access data, resulting in a "piecemeal" (or scattered) view that can miss critical overlaps or gaps in access rights.

Without a unified perspective, conducting thorough user access reviews becomes challenging, potentially leaving the organization exposed to risks of unauthorized access and subsequent data breaches.

The siloed nature of information across platforms complicates the review process. Also, it increases the administrative burden on IT and security teams, making it harder to identify and rectify vulnerabilities efficiently.

Solution:

- Deploy IAM tools with cross-platform capabilities.
- Invest in access governance software that provides visibility into user access rights and automates the monitoring and managing of these permissions.
- Develop or utilize API integrations between disparate systems and applications to facilitate the sharing of access data, creating a more integrated security architecture.
- Implement federated identity management practices to enable single sign-on (SSO) across different ystems, simplifying access control and visibility.

Dissatisfaction Due to Access Changes

It's not uncommon for employees to be dissatisfied with changes to their access rights. This is to be expected when access to previously available resources is restricted or when there are delays in granting necessary permissions. It can often lead to frustration among employees, potentially affecting their productivity and morale.

The key to mitigating these issues lies in managing access changes with sensitivity and ensuring transparent communication about the reasons behind such modifications. It's crucial for organizations to strike a balance between maintaining robust security measures and supporting the operational efficiency and satisfaction of their workforce.

Solution:

- Implement structured communication protocols to inform employees about changes to their access rights and the reasons behind these changes, emphasizing the importance of security.
- Offer a straightforward process for employees to request access rights reviews or adjustments, ensuring they have a medium to express their needs and concerns.
- Conduct regular training sessions to educate employees about security policies, the significance of access controls, and how they contribute to the organization's overall security posture.

Meeting Strict Compliance Requirements

Regulatory standards are continually evolving, each imposing specific demands on how access should be controlled and reviewed. This approach makes user access reviews important, serving as a means to demonstrate adherence to these regulations.

However, the challenge lies in meeting the requirements of each compliance standard. Failure to align user access review processes with these regulatory requirements can lead to non-compliance risk, potentially resulting in significant penalties, legal repercussions, and damage to an organization's reputation.

Solution:

- Stay Informed on Regulatory Changes: Regularly update knowledge bases and practices to reflect the latest regulatory requirements, ensuring that UAR processes remain compliant.
- Leverage compliance frameworks as guidelines for structuring UAR processes, ensuring that all regulatory bases are covered.
- Maintain detailed records of UAR processes, findings, and corrective actions, ensuring that documentation is readily available to demonstrate compliance during audits or regulatory reviews.

Recommended → Automating Compliance Controls to Achieve Least Privilege Access

High Employee Turnover

Each time an employee leaves, changes roles, or is newly hired, there’s a critical need to update access permissions accordingly. This requirement places additional pressure on IT and security teams, which may already be operating under considerable constraints.

This is to be expected as the nature of workforce changes can result in delays or oversights in revoking access for former employees, potentially leaving open pathways for unauthorized access.

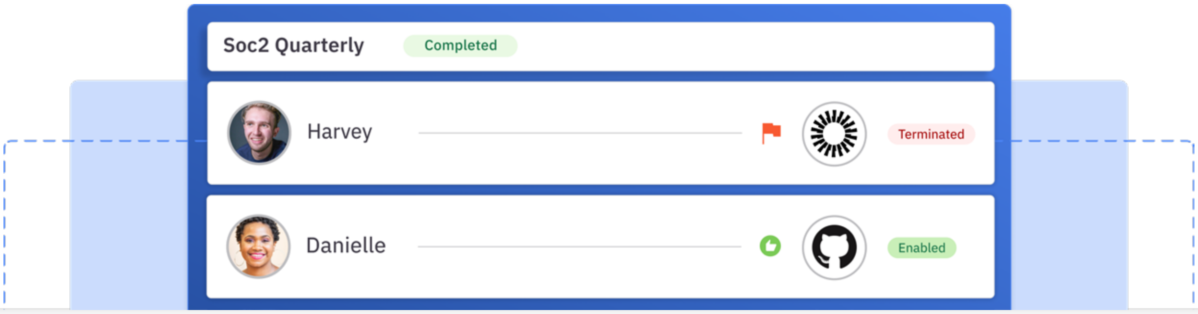
Similarly, delays in provisioning access to new hires can impede the efficiency and productivity of the workforce, as employees may be unable to access the resources they need to perform their duties.

Solution:

- Automate the onboarding and offboarding processes to streamline the granting and revocation of access rights as part of employee lifecycle management, reducing delays and the risk of oversight.
- Integrate HR systems with IAM solutions to automatically trigger access changes based on HR status updates, such as role changes or employment termination.
- Conduct frequent and systematic user access reviews to ensure access rights remain aligned with current job roles and promptly identify and rectify inappropriate access rights.
- Align access rights with job roles to reduce complexity in the UAR process.

Automate User Access Reviews with ConductorOne

ConductorOne is a comprehensive identity security and access control platform designed to secure an organization’s environment. The platform integrates with cloud infrastructure, SaaS, directories, data warehouses, HR systems, on-prem tools, and non-cloud infrastructure like LDAP, Postgres, Microsoft SQL, Active Directory, and more. It also supports integration with back-office or homegrown apps using ConductorOne’s Baton SDK.



Key Features of ConductorOne

Automated Access Reviews

Streamline the process of verifying user access rights with ConductorOne's automated reviews. This product significantly reduces manual workload, ensuring compliance and maintaining up-to-date access privileges across your organization.

With ConductorOne's automated access reviews, you get:

- Off-the-shelf integrations with applications allowing for fully automated reviews and notifications via email or Slack.
- Risk insights and context around usage, risk level, and flags related to job title, department, and anomalous access for better decision-making.
- Configurable review workflows to meet specific security needs, including multiple reviewers and delegated reviewers for absences.
- Streamlined certifications for automatically approving low-risk access and utilizing bulk approvals for efficiency.
- Easy revocations through automatic deprovisioning or manual revocation workflows.
- Full audit trail with population reports, access certification results, and remediation activity fully tracked for auditors, with one-click reporting.

Integrations

ConductorOne's integrations helps you streamline identity and user access data management across any SaaS, on-prem, cloud infrastructure, or hosted infrastructure system. These integrations are off-the-shelf, no-code setups that are operational in minutes, offering real-time visibility into fine-grained permissions, roles, groups, resources, and more.

With out-of-the-box integrations, organizations can:

- Gain visibility into roles, groups, and permissions across systems.
- Automate access controls for accounts, roles, and fine-grained entitlements.

Pro Tip → ConductorOne supports over 100 connectors for major SaaS apps, directories, databases, and cloud infrastructure providers, enhancing access governance for sensitive applications.

🔑 Baton

ConductorOne's Baton connectors offer access control for private apps and infrastructure, enabling organizations to enforce access control on their on-prem or private applications and infrastructure.

Baton's core elements include:

- Prebuilt open source connectors for popular SaaS, IaaS, and infrastructure to facilitate integration.
- SDK to build your own connector to any app or infrastructure.
- CLI for interacting with connectors and managing data efficiently.

With Baton connectors, organizations can:

- Gain visibility into roles, groups, and permissions across systems.
- Automate access controls for accounts, roles, and fine-grained entitlements.
- Discover identity-based risks, such as accounts without multi-factor authentication (MFA).

💡 **Pro Tip →** Baton enables integration with custom, homegrown, or back-office applications that aren't supported natively. Baton connectors and SDK can be used independently or alongside ConductorOne to add custom sync, discovery, or provisioning logic, audit behavior, or limit the scope of data transferred.

🔑 Access Controls

ConductorOne provides a unified solution for automating application and resource access controls across your environment using a centralized platform.

Benefits include:

- Users can request access from a customized catalog of permissions available to them using Slack or the web app.
- Users can create policies to remove access based on time, non-usage, or changed justification, orcing a re-request for especially risky access.
- Risk indicators are surfaced based on identity and permission levels to aid in making secure access decisions.
- Approval workflows can be configured to meet security needs, with delegated reviewers for absences and auto-approval for low-risk access.

🔑 Access Copilot

ConductorOne's Access Copilot redefines identity governance by leveraging the power of AI to surface risk-based recommendations and streamline access control. This solution is designed to help "human-in-the-loop" approvers with the right context for making informed access decisions, offering a seamless experience through existing helpdesk systems.

Key benefits include:

- To ensure informed decision-making, Copilot guides end users with recommendations based on risk factors, including existing access, previous access decisions, and more.
- Copilot surfaces insights such as usage, risk level, and anomalies related to job, department, role, and assigned permissions.
- Copilot flags downstream access implications for groups and resources, enabling teams to make the best decisions regarding access rights.
- The system can connect to your ticketing system to automate the creation and processing of access requests from helpdesk tickets, enhancing efficiency and accuracy.

🔑 Access Fabric

ConductorOne's Access Fabric enables organizations to visualize access paths, identify risky access, and remediate issues with just a click, significantly enhancing security posture and compliance.

Key benefits include:

- A comprehensive view of access risks such as orphaned accounts, inactive users, high-risk users, and unused permissions.
- Built-in remediation options include downgrading access, offboarding accounts, and securing service accounts, facilitating swift action to secure the environment.
- The ability to visualize access paths for any user, application, or resource to gain a clear understanding of effective access and fine-grained permissions.
- Powerful search capabilities for quickly answering identity-, authorization-, and access-related questions.

Why Choose ConductorOne For Your User Access Review Software?

ConductorOne

Certified

ConductorOne offers a powerful blend of automation, compliance, and security, streamlining the traditionally complex and time-consuming task of managing user access rights across various systems and applications

The platform automates the review process, reducing the manual effort required to track and manage access rights. This automation speeds up the review process and minimizes human errors, ensuring a more accurate and efficient audit of user permissions.

ConductorOne's provides comprehensive visibility into who has access to what within the organization. This visibility is crucial for identifying and mitigating potential insider threats and ensuring access rights adhere to the principle of least privilege.

Secure your company with unified access visibility, just-in-time access, self-service requests, and automated access reviews—all from a single platform.

Get a demo today

User Access Reviews: Process & Best Practices Checklist

ConductorOne | team@conductorone.com

AICPA SOC