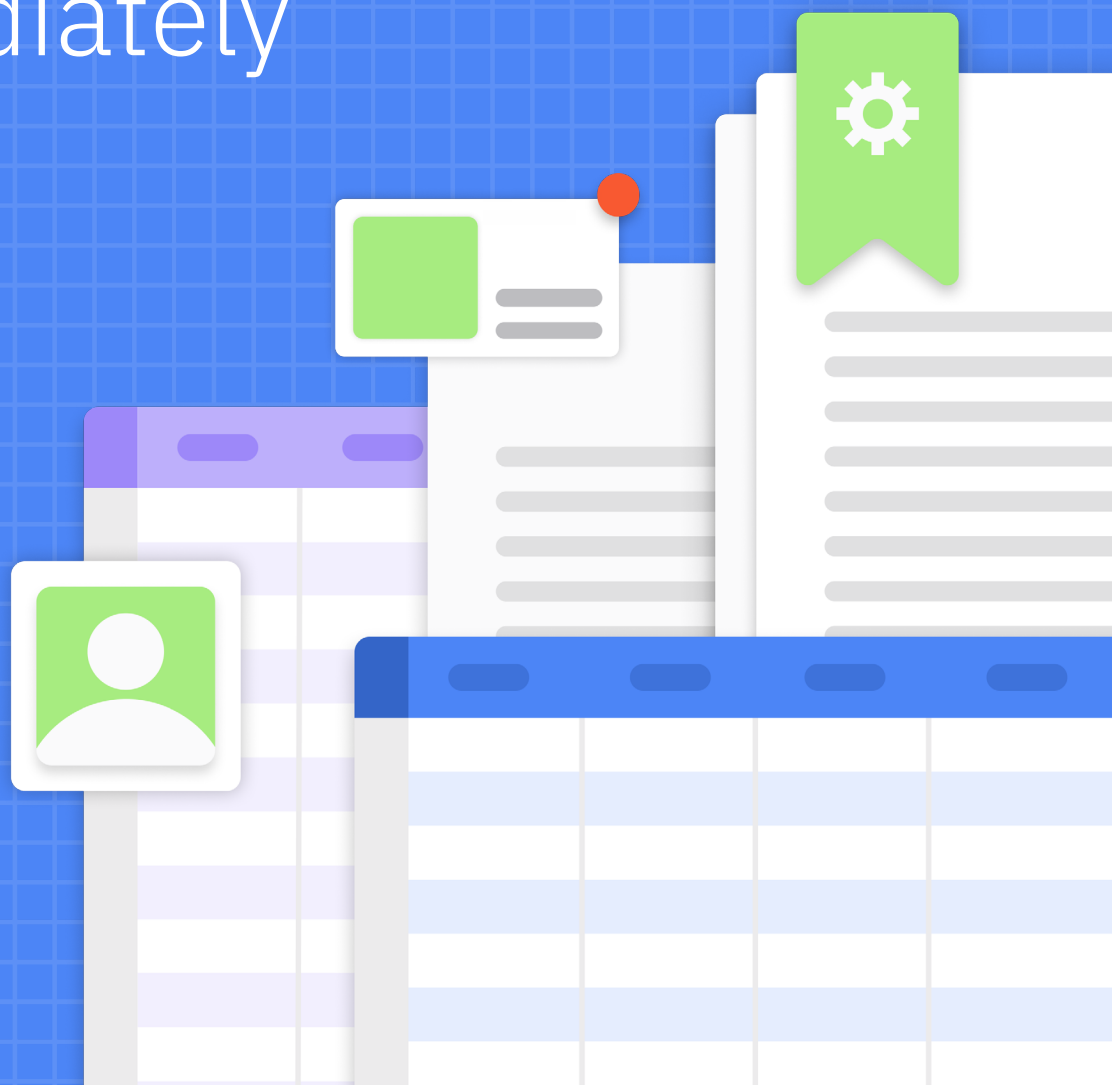


User Access Review Templates: Key Components and Examples You Can Use Immediately



Maintaining a strong security posture demands constant vigilance, and user access reviews (UARs) are a crucial part of that effort. A user access review template provides the framework for a systematic and repeatable process to ensure that access rights are appropriate, up-to-date, and compliant with security policies and industry regulations.

In this guide, we'll explore how user access reviews help organizations enhance security, minimize risk, and ensure compliance, along with providing actual templates you can download and use.

What is the purpose of user access reviews (UARs)?

User access reviews are essential to protecting your organization. Here's why:

- **Complexity is your enemy:** Modern organizations are complex. Employees change job roles, departments restructure, and new technologies are constantly adopted. Without a structured approach, it's incredibly easy to lose track of who has access to what. This creates a breeding ground for security vulnerabilities.
- **Compliance is nonnegotiable:** Regulations like [SOX](#), [GDPR](#), [HIPAA](#), and PCI DSS mandate regular user access reviews. These aren't just suggestions; they're legal requirements with serious consequences for noncompliance, including costly penalties.
- **Proactive security is essential:** The threat landscape is constantly evolving. Insider threats, data breaches, and cyberattacks are a constant reality. User access reviews help you proactively identify and mitigate these risks by ensuring that only authorized individuals have access to sensitive data and systems.

Ultimately, conducting regular user access reviews is about more than just checking boxes. It's about building a security-conscious culture, minimizing risk, and protecting your organization's most valuable assets.

The benefits of using a user access review template

- **Enhanced security:** Regular, systematic user access reviews identify and eliminate security gaps arising from outdated or unnecessary access privileges. Taking a proactive approach strengthens your defenses against security breaches, insider threats, and unauthorized access, safeguarding your critical assets and sensitive information.
- **Effortless compliance:** Meeting regulatory requirements like [GDPR](#), [HIPAA](#), or [SOX](#) becomes significantly easier. A template provides a documented and auditable process for demonstrating compliance, reducing the risk of penalties and reputational damage.
- **Increased efficiency:** Streamlining your access review process frees up valuable time and resources, allowing your IT and security teams to focus on strategic initiatives that drive business growth.
- **Reduced operational costs:** Minimize the risk of security incidents and compliance violations that can lead to financial losses. A proactive approach to access management helps avoid costly remediation efforts and legal battles.


Your complete user access review toolkit: 3 essential templates

Conducting regular user access reviews is a critical practice for organizations seeking to mitigate security risks and ensure compliance with industry regulations. However, disorganized data collection and certification processes and a lack of proper documentation can hinder the efficiency and effectiveness of these reviews.

This user access review toolkit is designed to streamline the review process. These templates provide a structured framework for conducting comprehensive access reviews, enabling organizations to enhance security, ensure data protection, improve compliance, and reduce administrative overhead.

Access review campaign template

This template provides a centralized spreadsheet for managing all access certifications and revocations within a user access review campaign. It facilitates efficient tracking and documentation of access changes, ensuring a comprehensive and auditable record of the review process.


 **How to use this template** — Each row of the access certification should be populated based on in-scope entitlements (group memberships, roles, etc.). Once certifications are completed, revocations or access changes should be executed and tracked.



[Download campaign template](#)

Application population report template

This template streamlines the generation of population reports from various systems, providing a consolidated view of user access across the organization. This facilitates the identification of potential risks and ensures that all users are included in the review process.


 **How to use this template** — Populate application population reports for each system that's in scope prior to kicking off access reviews. You will also need to ingest HR and/or cloud directory data to map app users. This ensures that you have a complete picture of user status so that you can identify the corporate identity responsible for the local user account and find the manager for that user if needed.



[Download population report template](#)

Notifications template

This template offers preformatted email communications for notifying reviewers about pending review tasks and overdue actions. Sending regular notifications ensures timely completion of reviews and reduces the risk of missed deadlines.

 **How to use this template** — Copy the appropriate communication template, add and remove language where needed, and send to reviewers.



[Download notification template](#)

The user access review process: 6 key steps

Here's a breakdown of the key steps involved in conducting regular user access reviews:

1. Planning and scoping

- **Identify in-scope systems:** Determine which applications, systems, and data repositories will be included in the review. Prioritize critical systems containing sensitive data and those subject to regulatory compliance.
- **Define entitlements:** Clearly define the access rights, user roles, and user permissions that will be evaluated for each system. This includes identifying different levels of access (e.g., read-only, read-write, admin).

2. Data gathering

- **Pull data from in-scope systems:** Gather identity and access data from in-scope applications, user directories, and HR systems
- **List all users:** Include internal employees, external partners, and terminated users.
- **Document each user's access:** Document the access users have to in-scope systems, noting their roles (admin or user) and any access to privileged accounts.

3. Analyzing user access

Review the collected data to identify potential risks:

- **Terminated employees and third-party vendors:** Ensure that accounts of former employees and external partners are deactivated and their access revoked. Update offboarding processes to prevent future oversights.



- **Shadow admin accounts:** Identify non-admin accounts with sensitive privileges (shadow admins). Revoke unnecessary privileges or move these accounts to a privileged admin group for closer monitoring.
- **Privilege creep:** Identify employees who have changed roles and may have accumulated excessive permissions (privilege creep). Remove any access no longer required for their current responsibilities.
- **Unnecessary access:** Review the remaining users to ensure they have only the necessary access and privileges to perform their job duties.

4. Generating Access Certification

Access certification is a critical step in the user access review process. It involves creating a detailed record of user access privileges across all relevant systems and applications. This record should clearly outline the applications they can access, their roles and permissions within those applications, and any specific data they can access. This information should be organized in a clear and concise format, ensuring [completeness and accuracy](#).

This step is crucial because it establishes a clear baseline of each user's current access privileges, facilitating an efficient and accurate review process. By having a structured overview of user access, reviewers can easily assess whether those permissions are appropriate and aligned with the [principle of least privilege](#). Access certifications also serve as auditable documentation, supporting compliance with regulatory requirements and demonstrating a commitment to robust security measures.

5. Reviewing and approving

- **Federate to reviewers:** Assign access certifications to appropriate reviewers, such as data owners, application owners, line managers, or IT security personnel.
- **Review and make decisions:** Reviewers evaluate each access certification and decide to approve, revoke, or modify access based on the principle of least privilege, security policies, and compliance requirements.

6. Remediation and monitoring

- **Remediate access:** Implement the approved access changes, including revoking unnecessary permissions, modifying access levels, or disabling inactive accounts.
- **Downgrade permanent access:** Evaluate whether users with permanent access can be downgraded to temporary access when appropriate.
- **Document changes:** Maintain detailed documentation of each review cycle, including the list of tools, user access rights, reviewer comments, approver decisions, and any access changes made. This ensures transparency and simplifies future reviews.
- **Monitor and track:** Continuously monitor user access and activity to detect anomalies and ensure ongoing compliance.

The duration of a user access review can vary depending on factors like the number of systems, the complexity of access rights, and the level of automation used. Typically, reviews can take anywhere from 2 to 8 weeks to complete.

Simplify user access reviews and enhance your organization's cybersecurity with ConductorOne



Maintaining a strong security posture and ensuring compliance requires efficient and thorough user access reviews. However, traditional manual processes can be time consuming, error prone, and challenging to scale.

ConductorOne simplifies and automates user access reviews, empowering your organization to:

Streamline the review process

- **Centralized access management:** ConductorOne provides a [unified platform](#) for managing user access across all your cloud and on-prem applications and systems. This centralized view simplifies the review process and eliminates the need to navigate multiple tools and dashboards.
- **Automated workflows:** Automate every step in the review process, including data scoping and collection, risk analysis, reviewer notifications, and proof of data accuracy. This reduces manual effort and ensures consistent and timely reviews.
- **Intuitive dashboards:** Gain clear visibility into user access with intuitive dashboards and reports. Quickly identify potential risks, track review progress, and demonstrate compliance.

Enhance collaboration and efficiency

- **Automated notifications and reminders:** Keep reviewers informed and engaged with automated notifications and reminders in Slack and email to ensure timely completion of reviews and reduce delays.
- **Easy collaboration:** Facilitate seamless collaboration between reviewers, stakeholders, and IT teams directly in Slack.

Strengthen security and compliance

- **Continuous tracking:** ConductorOne continuously tracks user access and usage activity, providing real-time alerts for high-risk access and [separation of duties](#) violations.
- **Automated remediation:** Enforce security policies and compliance requirements with automated remediation capabilities. Automatically revoke or modify access based on predefined rules and risk profiles.
- **Comprehensive audit trails:** Maintain detailed audit trails of all access changes and review activities. This ensures accountability and simplifies compliance audits.

ConductorOne's modern identity governance platform helps you:

- **Reduce security risks:** Implement proactive [access controls](#) and identify and mitigate potential vulnerabilities before they lead to breaches.
- **Improve compliance:** Meet regulatory requirements with [fully automated access reviews](#) and detection of access conflicts.
- **Increase efficiency:** Streamline workflows and free up valuable time for your IT and security teams.

Ready to simplify and automate your user access reviews? [Talk to our team.](#)

FAQs

What is a periodic user access review?

A periodic user access review is a systematic process of evaluating and verifying whether users have appropriate access privileges to organizational systems, applications, and data. Periodic reviews are conducted regularly (e.g., quarterly, annually) to ensure that access rights align with current job responsibilities, security policies, and regulatory requirements.

During a user access review, designated reviewers assess each user's access and make decisions to:

- **Approve:** Confirm that the user's current access is appropriate.
- **Revoke:** Remove access that is no longer needed or authorized.
- **Modify:** Adjust access levels to align with the user's current role and responsibilities.

Who should do user access reviews?

The responsibility for conducting user access reviews typically falls on a combination of individuals:

- **Data owners:** Individuals responsible for the security and integrity of specific data sets. They have the authority to determine who should have access to the data.
- **Application owners:** Individuals responsible for managing and securing specific applications. They understand the access requirements for their applications.
- **Line managers:** Managers who supervise employees and have insight into their job responsibilities and access needs.
- **IT security teams:** The IT security team plays a crucial role in facilitating the review process, providing tools and support, and enforcing security policies.

User access review best practices

- **Establish a clear policy and scope:** Define a comprehensive policy that outlines the frequency, scope, and roles and responsibilities for user access reviews. This policy should align with your organization's security standards, such as ISO 27001, and regulatory requirements.
- **Automate where possible:** Leverage automation tools to streamline data gathering, analysis, and reporting. This reduces manual effort, improves accuracy, and allows for more frequent reviews, strengthening your internal controls.
- **Implement role-based access control (RBAC):** Utilize [RBAC](#) to simplify access management and ensure that users have the appropriate access permissions based on their roles. This helps prevent privilege creep and streamlines the review process.
- **Focus on risk:** Prioritize high-risk users and systems. Focus your efforts on users with elevated privileges, access to sensitive data, or those who have undergone recent job changes. Consider implementing risk-based authentication to further enhance security.
- **Engage stakeholders:** Clearly communicate the importance of user access reviews to all stakeholders, including business unit managers, data owners, and IAM providers. Provide training to reviewers and foster collaboration between IT and security teams.

- **Maintain documentation:** Keep detailed records of all access review decisions and maintain comprehensive audit trails. This documentation supports compliance efforts and provides valuable insights for future reviews and audits.
- **Continuously improve:** Regularly evaluate the effectiveness of your user access review process and make adjustments as needed to optimize its efficiency and alignment with industry best practices and evolving security threats. Consider automating user [provisioning and deprovisioning](#) processes to improve efficiency and reduce errors.

Want to learn more about our identity security platform for modern workforces?

Get a demo