CYBERARK®
THE IDENTITY SECURITY COMPANY®

Compliance Whitepaper

The Definitive Guide to User Access Reviews

2025

Introduction to User Access Reviews

User Access Reviews (UARs) are periodic checks of the levels of access that users in an organization have to particular assets — such as systems, data, and applications. This is the intersection between the following:

- **Users** – including employees, contractors partners, and also service accounts and other machine identities
- **Assets** – including computer systems, data, applications, and other resources
- **Permissions** – rights or entitlements to perform various actions, such as viewing, changing, or deleting information or capabilities

The goal of the UAR process is to:

- Centrally collect and collate all existing permissions for an in-scope set of application, users, or privilege types
- Have all permissions reviewed by the most appropriate person in the organization to identify any permissions that are excessive or not job-appropriate and need to be revoked
- Complete and document the process of reviewing all permissions and revoking inappropriate permissions

Typically, a UAR is initiated on a periodic basis and involves a team of people, typically a governance team and various stakeholders across the business. Together they uncover existing permissions, ensure the permissions are properly understood, present them to a person with knowledge (often supervisors business owners across the organization) of what they should be, and allow for review and correction. They also gather and incorporate evidence regarding the permissions and any changes that were made.

The drivers for a UAR come from the realms of both compliance and security. Fundamentally, you can't have confidence in the *validity* of data unless you know it has appropriate controls around who can create, modify, and delete it. Similarly, you can't have confidence in the *privacy* of the data unless you know it has appropriate controls around who can view and transmit it.

From the compliance perspective, there are many standards that may automatically apply to an organization and thus prompt a UAR. Some of the most common standards include the following:

Sarbanes-Oxley Act (SOX) – a regulation applicable to publicly traded companies doing business in the United States that's designed to help ensure accuracy and transparency in their accounting.

Payment Card Industry Data Security Standards (PCI-DSS) – a set of rules identifying steps that companies need to take to provide for the security of cardholder data.

General Data Protection (GDPR) – a set of regulatory requirements established by the European Union (EU) to control how companies handle personal data of their employees and customers.

Digital Operational Resilience Act (DORA) - a regulation introduced by the European Union to strengthen the digital resilience of financial entities, including banks and insurance companies. It establishes a standardized framework for managing risks related to information and communication technology (ICT) in the financial sector.

California Consumer Protection Act (CCPA) – similar to GDPR, CCPA establishes rules for the proper handling of personal data of California residents.

Health Insurance Portability and Accountability Act of 1996 (HIPAA) – a set of regulations governing how organizations handle personal medical information. It covers medical organizations of all types, including insurance providers or anyone else who gathers, stores, or processes this data.

In addition, there are many standards that an organization may wish to comply with to demonstrate their security posture and data protection activities to customers and partners. These include the following:

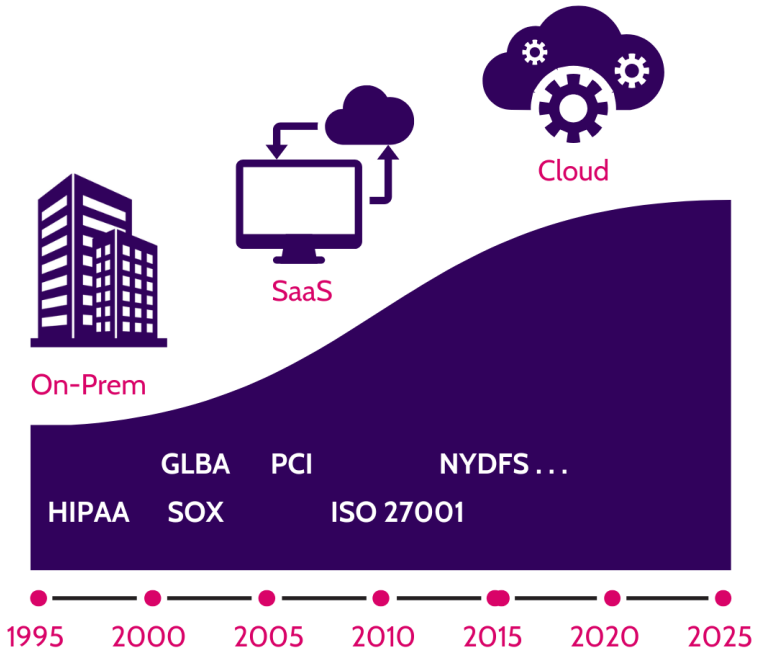
International Organization for Standardization (ISO) – a set different guidelines including those, such as ISO 27000, focused on information security.

SOC (System and Organization Controls) 2 – a compliance framework for evaluating controls regarding the safety, availability, confidentiality, and integrity of a system. Cloud computing providers, SaaS companies, and analytic firms typically need a SOC 2.

National Institute of Standards and Technology (NIST) – provides tools such as the NIST Cybersecurity Framework (CSF) that describe guidance for organizations to manage and reduce cybersecurity risks effectively. NIST also publishes SP 800-53 within information about security and privacy controls for information systems, which includes account management, access enforcement, separate of duties, least privilege, and other controls relevant to a UAR.

The Growing Need for User Access Reviews

User Access Reviews (UARs) are increasingly important because both main drivers — compliance and security — are on the rise. In fact, according to the [2025 State of IGA Survey Report](), 91% of identity leaders have experienced



an increase in the scope of UARs in the just the past three years, with 84% believing that the increase will continue for the next three years as well.A good example of the steady increase in compliance drivers is NYDFS — the New York Department of Financial Services standards. These are being rolled out in several phases starting in 2024 and 2025, and they apply to financial services institutions operating in New York. That includes banks, mortgage companies, insurance companies, and more. A key aspect of this is the requirement, starting in 2025, that organizations conduct annual user access reviews along with associated remediation activities. Organizations also need to implement multi-factor authentication (MFA) for remote access and for access to privileged systems. For more information, see https://zillasecurity.com/blog/guide-to-nydfs-compliance-how-zilla-can-help/.

Information security provides the other primary driver for UARs. The most important cyber attack vectors in recent years have involved identities. Attackers most commonly obtain a toehold within an organization by compromising one or more accounts, then they escalate their privileges to access critical data or compromise critical systems and applications. These attackers take advantage of weaknesses such as:

- User accounts which are active even though the employee is no longer with the organization
- Accounts with excessive privileges — from user error or maybe as a result of a change in position that wasn't accompanied by changes in permissions
- Accounts that should have MFA enabled but that don't
- Access from a partner organization that isn't properly maintained
- Machine user accounts with credentials that are left exposed

These are real-world issues, as illustrated by the finding in the 2025 State of IGA Survey Report that more than half of organizations uncover an orphaned or excessive permission rate exceeding 10% of all their entitlements. In each of the weaknesses above, an effective UAR program can help uncover and remediate issues in the organizational identity security posture that could lead to compromise.

Different Types of UARs

In addition to the different drivers for User Access Reviews — various compliance and security goals — there are also different types of UARs, with each one answering different questions that correspond to the driver.

The list below isn't intended to cover every potential type of UARs, but it does include the most common ones.

Privileged Users | Full Time Employees | Contractors | Terminated Employees | Transferred Employees | Shared Accounts | Inactive Accounts

Periodic Access Reviews – These are regularly scheduled reviews (e.g., quarterly or annually) encompassing a defined base of users. They verify that user access is still appropriate based on roles or responsibilities.

Privileged Access Reviews – These focus on users with elevated or administrative access to ensure that each one requires such permissions.

Terminated Employee Access Reviews – These reviews focus on employees that have left the organization, to make sure that their account access has been fully revoked.

Transferred Employee Access Reviews – These reviews cover employees who have changed roles within an organization ("movers"). They look for old access that should have been revoked as well as for access that could compromise segregation of duties (SoD) or is generally inappropriate.

Inactive Account Reviews – Similarly, these reviews take the perspective of user activity and look to revoke access for accounts that haven't been used for a specified period of time.

Separation of Duties Reviews – These ensure that no single user has conflicting access privileges that could lead to fraud or security risks (e.g., both processing and approving payments).

Application-Specific Access Reviews – These reviews are essentially "deep dives" into a particular system or application, looking for excessive or outdated permissions.

Ad-Hoc Reviews – These are reviews that are conducted in response to specific events, such as a security incident, to verify and adjust user access as needed.

These reviews play a critical role in safeguarding sensitive information and maintaining an organization's overall security posture, ensuring that access is job-appropriate and follows the principle of least privilege.

Why UARs are Challenging

Despite the value in a thorough UAR, there are challenges in implementing one with the least amount of cost and organizational disruption. These challenges include the following:

- **Scale** – Many organizations have large numbers of employees, applications and systems, and many different kinds of permissions. The increasing use of machine identities also adds to scale.
- **Rate of change** – A significant proportion of the user base joins, leaves, or changes role in a given year. New systems and applications are added, while old ones are decommissioned. New types of entitlements can also be added to existing applications and systems. The UAR environment is highly dynamic.
- **Inconsistent data** – Data about employees, systems, applications, and permissions are often stored in inconsistent ways, making it very difficult to cross reference the data.

- **Distributed knowledge** – While there are some definitive systems of record, even those aren't managed and maintained by a single group within an organization. Definitive lists of employees, along with titles and reporting information, are managed by HR. Lists of systems are often maintained by IT. With the rise of SaaS, comprehensive lists of applications can be scattered throughout an organization. And certainly, knowledge about permissions will be distributed — applications each have their own set of permissions that are often unintelligible to anyone except for application owners. As a result, extensive coordination is needed to perform a UAR.
- **Rigorous process and documentation requirements** – As background to the above, there's the issue of following a process which is rigorous and which needs to be documented every step of the way. Not only must an organization execute UARs properly, it needs to generate convincing and thorough evidence that can be reviewed by the necessary authorities, including both internal and external auditors.

Meanwhile, UAR challenges are multiplied by the number of compliance obligations. The 2025 State of IGA Survey Report indicated that 55% of identity leaders are required to perform UARs for five or more compliance obligations. And almost a fifth perform UARs for 11 or more obligations. So it's no wonder that 39% of respondents in the survey said they struggled with the effort to manage the growing scope of UARs.

Executing an Effective and Efficient UAR

Completing an effective and efficient UAR means addressing each of the challenges outlined above. Often, many different groups within an organization need to be involved, their activities need to be coordinated, and automation is a necessity if UARs are to be accomplished reliably and efficiently. Yet 84% of organizations rely heavily or entirely on manual processes. To address the challenges of a UAR, the following best practices are important to keep in mind.

Best Practice 1: Addressing IT Decentralization

Decentralized IT, which is often driven by the proliferation of cloud and SaaS in the enterprise, results in fragmented data and broad ownership of systems and applications. To make sure they have thorough, robust IT coverage, organizations can:

- **Standardize Data Management:** Implement a single governance process and framework that sets clear, uniform procedures for data management and audit preparation across all departments. The process and framework should include clear guidelines on documentation, data collection methods, and reporting formats to ensure consistency.
- **Leverage Automation Tools:** Use modern automation tools that integrate with a wide range of systems and platforms to help streamline the collection and analysis of data from disparate sources. This reduces the potential for human error and ensures that audit processes are both thorough and efficient.
- **Simplify Audit Processes:** Create and adopt non-disruptive audit processes that all departments can follow. This includes developing easy and automated methods for data collection, standardized campaigns, and uniform criteria for collecting and evaluating the results. Ideally, your process should not

interfere with your stakeholders' normal business operations.

- **Require Ownership and Accountability:** To ensure a clear line of responsibility for data management and system controls, it's essential to define and communicate the roles and responsibilities associated with data and system ownership across the organization. This clarification helps guarantee that every department and individual understands their role in managing and safeguarding data, as well as in providing timely and accurate information during audit preparations.

Best Practice 2: Ensuring Data Integrity

To clearly demonstrate adherence to regulatory standards, organizations need to capture and export data meticulously.

- **Standardized Reports:** Standardization ensures that data is captured in a consistent format, making it easier to compare and analyze. This consistency is critical for auditors to verify the accuracy of the data and to ensure that all relevant information has been included in the audit.
- **Timestamping:** Timestamps serve as a vital piece of audit evidence, providing a clear and indisputable record of when data was extracted. This practice not only enhances the credibility of the data but also helps in establishing a timeline of events, which is crucial for tracking changes and identifying potential issues within the IT environment.
- **Audit Trails:** Organizations should prioritize solutions that offer clear, transparent audit trails. They should cover both automated and manual steps, for example using before-and-after screenshots. These trails are essential for verifying the authenticity of the data and for tracing any issues back to their source. They also can verify the automation process itself, providing a record of all actions taken by the tool, including data captured, reports generated, and changes implemented. Additionally, direct integration capabilities with a wide range of applications and systems ensure that data can be accurately and efficiently collected from all relevant sources.

Best Practice 3: Enhancing Accuracy Through Automation

Automated tools can facilitate direct data extraction from systems, bypassing the need for intermediate and manual steps that could compromise data integrity. Repetitive tasks, such as data extraction, report generation, and access reviews, are particularly susceptible to mistakes when performed manually. Many organizations struggle with this, as we can see from the 84% of organizations in the **2025 State of IGA Survey Report** that rely heavily or entirely on manual processes.

Automation streamlines UAR processes, ensuring that actions are performed consistently and accurately every time. It can also support the automation of various functions beyond data collection, such as initiating access reviews, sending reminders, and executing access changes based on review outcomes.

Organizations should Incorporate a campaign readiness stage into their automated UAR process. This ensures all data, permissions, and user accounts under review are up-to-date and accurately represented before initiating the formal review process. It includes:

- **Verification of Current Data:** Conducting a thorough verification ensures that all applications, user accounts, and associated permissions included in the review are current. This step is crucial for ensuring that reviewers assess the most accurate and recent information.
- **Updating Business Context:** The number of entitlements within applications continues to rapidly proliferate. And, as applications evolve, so do their associated permissions. Providing accurate and comprehensible descriptions of permissions helps reviewers make informed decisions. Clear descriptions demystify complex permissions, ensuring that reviewers understand exactly what they are approving or revoking.
- **Correct Mapping of Accounts to Users:** A common challenge in access reviews is ensuring that user accounts are correctly mapped to the individuals using them. The Campaign Readiness stage is a time for organizations to meticulously verify these mappings.
- **Correct Reviewer Assignment:** It's also important that the right reviewer is assigned for each user/account and application. An automated tool can help both initially and as any reassignments are needed.
- **Preparation of Audit Evidence:** This stage also involves preparing and compiling all necessary audit evidence to support the review process. This may include before and after screenshots of application settings, logs of the review process, documentation of compliance controls, or any other evidence required by auditors.

Another important aspect of automation is related to applications that don't support permission data retrieval via an API or by exporting permissions data into a CSV file. At CyberArk, for example, we have taken a unique approach to solving it through robotic automation. This feature, called Zilla Universal Sync (ZUS), retrieves user accounts and associated permissions from any app that doesn't support APIs or data exports. It creates recipes that learn how to collect data and then deploy these recipes automatically for ongoing permission data synchronization.

Best Practice 4: Establishing Trust in Automated Tools

For auditors and stakeholders alike, an automated tool has many advantages in terms of effort, reliability, and speed of execution. For any solution, however, the confidence in it hinges on clear, demonstrable proof that it provides an accurate record of the UAR process, including the following:.

- **Transparent Audit Logs:** Your audit logs should meticulously record every action performed by the tool, including data captures, report generations, and any access changes implemented. Providing a detailed account of the tool's activities enables auditors to verify the accuracy and integrity of the data being presented.
- **Data Immutability:** Ensure data immutability through tool features that prevent the modification of data after it has been captured. This guarantees that the data presented for audits remains unchanged from when it was originally captured.

- **Validation and Verification Processes:** Implement processes that involve cross-referencing tool-generated data with source systems to ensure consistency and accuracy. Presenting auditors with evidence of these validation checks allows them to assess the tool's effectiveness in accurately capturing and maintaining data.

Best Practice #5: Thoughtfully Determine the Right Scope and Frequency

A UAR is really part of a program to mitigate risks that arise over time from user oversights and escalating privileges for the sake of productivity. There's a fundamental cost/benefit tradeoff here. Execute a UAR every week and you almost completely eliminate risk, but the costs are unbearable. Execute a UAR every 5 years and there's almost no cost, but also almost no impact upon risk. Most organizations settle upon a frequency that balances cost and risk in a way that makes sense for them, keeping in mind that they need to meet the frequencies stipulated by the compliance standards, if needed. The resulting frequencies can vary depending on compliance standards, and the user groups and applications, resulting in UARs that are performed, for example, yearly, quarterly, or monthly.

Leveraging automation is a huge benefit in meeting an exceeding the required frequencies of your UARs.

Best Practice #6: Proactive Stakeholder Involvement and Education

It's important to thoroughly educate all relevant stakeholders about any new user access review processes or tools. This fosters trust and reliability from the outset. Internally, this may mean coordinating with internal audit teams, IT compliance teams, and application owners. Externally, this typically involves educating audit advisors and auditors about the process and tools, and explaining how tools are configured and used. Educating auditors and reviewers about new processes introduced by the organization can demonstrate the simplicity and efficiency of these new processes, proactively dispelling any potential concerns about their complexity.

Due to the resistance often encountered with any process changes, staff education should highlight how the new process streamlines reviews, reduces manual errors and contributes to a more robust compliance framework.

Delivering the Goods to Auditors

As indicated above, building a strong relationship with auditors earlier in the process is considered a best practice. It helps you can identify any gaps you may have and to understand what will be involved in the audit itself. This is important because once the audit begins, the situation is evaluative rather than collaborative, even though the auditor may wish the audit to go smoothly and have a satisfactory result.

User Access Reviews are an important part of an audit because they are a mitigating control. Roles and permissions established within systems, applications, and identity management systems are primary controls. However, there's lots of room for human error, and a UAR mitigates the risk of those errors in a timely manner.

For the auditor to be comfortable with the proper use of a UAR, they need to see evidence. You can think of this evidence in terms of the elements of a story, or a newspaper article — elements such as the who, what, when, and how. You want to provide auditors with the following types of information:

- **Who** – Who does the UAR? It should be who know the users and the applications.
- **What** – Exactly what data was reviewed? What groups, users within them, what applications, etc.?
- **When** – Exactly when was the UAR performed? Was the data extracted at the same time, and what's the evidence for that? How often are the UARs performed?
- **How** – Exactly how were any identified discrepancies handled? Exactly what is the evidence that issues were addressed (access updates were performed) immediately?

Providing lists of users pulled directly from relevant systems, with appropriate timestamps, is a good starting point. Then you should clearly document steps taken, actors, and time stamps — as would be tracked within a workflow system. Ideally you will show evidence such as before-and-after screenshots for updates that are made. While it's possible to collect and organize this information manually, for any substantial sized organization, an Identity Governance and Administration (IGA) solution that excels at UARs is a huge help.

Common Pitfalls in UARs

In addition to learning about how to execute a successful UAR, it's useful to consider the pitfalls that can arise. Success often hinges upon avoiding mistakes, and here are some of the most common.

Not including all the right applications – A UAR needs to include the right applications within its scope. While sometimes it isn't feasible, or even necessary, to include all applications, you need to cover those that impact the focus of the review. Aside from an audit, UARs for other purposes need to include those applications that are relevant to the situation, for example a compliance or security review.

Incomplete user coverage – The right user coverage is also critical to a UAR. Several common situations arise that are worth calling out:

Only reviewing terminated employees – Confirming that access for terminated employees has been removed is a critical part of a UAR. So is confirming that employees who changed roles have the right adjustments to their entitlements. But a UAR can't stop there; it needs to include all current in-scope employees. And it needs to also include contractors or other service providers that have organizational access.

Focusing too much on admins – Application administrators are a natural place to start when evaluating entitlements, since they have "the keys to the castle". However, it's not appropriate to ignore other, less privileged users. Some compliance requirements, such as HIPAA and GDPR, focus heavily on the privacy and integrity of the data, and so anyone with access to it — admin or not — is important. In other cases, there are important interplays between how non-privileged users interact with an application to cover requirements such as segregation of duties.

Ignoring service accounts – Service accounts need to be included in entitlement reviews, to make sure permissions are appropriate and current. These accounts are generally enabled with privileged access, posing a higher risk, and are particularly challenging to manage because they often can't take advantage of enhanced security measures such as multi-factor authentication (MFA) or Single Sign On (SSO). But service accounts can be more closely monitored to detect, for example, any interactive logins associated with the accounts, as those shouldn't ever occur. The first step in managing the governance of service accounts, as a best practice, is to associate each service account with a human owner that is responsible for it.

Shared accounts – Ideally there shouldn't be any shared accounts in an organization. But if they exist, those accounts need to be reviewed, and highly monitored as well.

Only reviewing the identity provider group-level access – Many organizations centralize their authentication and access control using an identity provider, such as Okta, Entra, or CyberArk Workforce Identity. They may limit their review of permissions to only the groups that an IdP creates to help inform access. A UAR certainly should include the identity provider, but **it's not enough to stop at the group level.** You still need to review the individual entitlements and applications themselves to make sure permissions and roles are correct. Only a review of the specific entitlements within an application will satisfy audit completeness and accuracy requirements, and a review of groups will not meet these criteria.

Permissions that are confusing and unclear – Every permission needs review, but this can't be done properly if the reviewer doesn't understand them. To address this, make sure you have the involvement of application owners in clearly describing the permissions, and ideally as well in helping execute the reviews.

Wasting reviewer time with repetitive tasks – Involving applications owners is important to performing a good UAR, but no one wants to review hundreds of the same basic access profiles – e.g. every seller needs basic access to SalesForce. **Pre-approval, which can be supported by AI**, can dramatically reduce the number of manual reviews required while still providing documentation needed for the auditors.

A Reactionary Approach to UARs – It's tempting to take a just-in-time approach to executing a UAR, for example in response to an audit or a security event. However, as described earlier, the frequency of UARs is important to determine in advance as part of a risk mitigation program. A last-minute or reactive UAR is a sign that the organization hasn't determined the right frequency for UARs, and that they have no fundamental process for mitigating the risks that UARs address. Or, if they do have a process, they're not following it.

Providing auditors insufficient detail – Auditors need to be comfortable with your process of executing a UAR, and the key to that is sufficient evidence. Just seeing a ticket saying, "Reviewed application X and it was OK", with no detail behind it, probably won't satisfy an auditor. You need to be able to illustrate the process you went through, providing a complete "story" that an auditor can follow.

CyberArk IGA – Your UAR Solution

CyberArk Comply is the most automated solution for User Access Reviews and enabling continuous audit-ready compliance. It has all the functionality you need to execute access reviews with 80% less effort:

- Fully automated campaign preparation, review management, and evidence creation.
- Integration with the broadest set of applications via extensive built-in support, API integration, and Zilla Universal Sync.
- Robotic automation for easily integrating with virtually any application or system for entitlement data.
- Coverage of both cloud and on-premises systems.
- Delegation capabilities so that knowledgeable app owners can fill in all of the permissions descriptions.
- Automated review campaigns that coordinate activities across all your application owners.
- AI Profiles to reduce manual reviewer efforts by up to 75%.
- Enforcement of least privilege access with real-time alerting of entitlement risks.
- Collection of all your review data into a comprehensive audit package that includes accounts, permissions, roles, groups, review workflow, applications changes/revocations with screenshots, etc.

For more information, including a UAR demo, see **https://zillasecurity.com/user-access-reviews/**