Common Pitfalls of User Access Reviews

CYBERARK

GUIDE

USER ACCESS REVIEWS – ESSENTIAL BUT CHALLENGING

User Access Reviews (UARs) are periodic checks conducted in organizations to ensure users have appropriate access to systems, data, and applications. UARs involve reviewing user permissions across employees, contractors, service accounts, and machine identities to determine whether their access levels are appropriate.

UARs are essential for both security and compliance:

- **Security:** Ensures data privacy and integrity by preventing unauthorized access.
- **Compliance:** Many regulations require organizations to conduct access reviews. These include, for example, **SOX** (Sarbanes-Oxley Act) for financial reporting accuracy, **PCI-DSS** for cardholder data security, **GDPR & CCPA** for personal data protection, **HIPAA** for medical data security, **DORA** for digital resilience in financial institutions, and **ISO, SOC 2,** and **NIST** frameworks for security best practices.

User Access Reviews (UARs) are increasingly important because both main drivers — compliance and security — are on the rise. However, they can be challenging to execute, because of organizational scale; constant changes in the user community and in applications; distributed knowledge about who should have access to what; and rigorous process requirements and documentation.

Completing an effective and efficient UAR means addressing each of those challenges. 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.*[1] To address the challenges of a UAR, the following best practices are important to keep in mind.

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

[1] Source: Zilla Security, 2025 State of IGA Report, January 2025

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.understands their role in managing and safeguarding data, as well as in providing timely and accurate information during audit preparations.

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 Modern IGA, Powered by Zilla – Your UAR Solution

CyberArk Modern IGA, Powered by Zilla, 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/