Best Practices for Executing an Effective and Efficient UAR

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.

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.

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

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 Zilla, 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.

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/