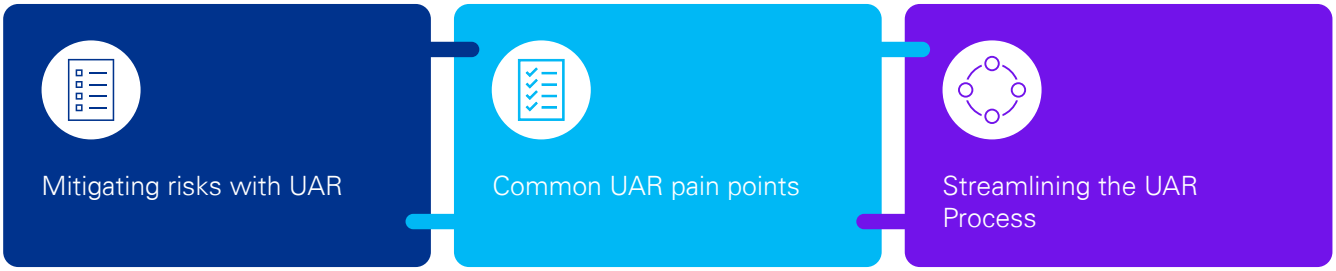
How to lessen the pain points of user access reviews

Application Risk Insights

As businesses accelerate their digital transformation, user access review (UAR) has become a major priority for modern enterprises to support their evolving workforce and customers. Once viewed as an operational back-office issue, UARs are now gaining board-level visibility to stay compliant and manage risks effectively.

However, managing UARs can be difficult, but by understanding their pain points organizations can put together a framework to help lessen their complexities and discover ways to improve the process.

The path towards effective UAR management



Mitigating risks with UAR

UAR is the process of periodically re-certifying the appropriateness of logical user access and security entitlements for production applications. Executing periodic UARs is a key control that verifies the adherence of user community to the risk-based principle of least privilege and ensures access is limited to the right users within the organization. A well-defined, documented UAR policy helps mitigate potential risks and control failures while providing auditable evidence for satisfying compliance requirements, such as SOX, which mandates firms to know who has access to secure data.

Addressing UAR risks

Inappropriate access rights can lead to malicious attacks and internal errors that may have a detrimental impact on a company's reputation and the bottom line. Some of the common access risks scenarios include:

- UARs provide insights into modifications or reassignments of security roles
- Detect terminated employees that have retained application access
- Identify separation of duties (SoDs) vulnerabilities
- When a terminated employee still has active user credentials that grant access to sensitive financial data

- Granting temporary approval access for invoices to a "backup" resource but failing to revoke it. The CFO, responsible for governing key financial reports, unexpectedly provisioned with broad transactional capabilities instead of "inquiry-only" access
- IT personnel, focused on application maintenance and environment setup, enabled with access to initiate G/L impacting transactions.

Common UAR pain points

It is taxing for companies to regulate admin privileges with cloud transformations. The difficulty of managing "who can access what" introduces new challenges to CIOs. Most of these user access risks do not exist in a vacuum, instead, they form complex relationship networks. The best way to optimize user accesses within an enterprise and prevent related risks is to prioritize the following pain points and promptly address them:

- **Process ownership**—Most often the best-equipped user does not own the UAR process. The functional leads or business process owners must be in-charge of conducting user access reviews and ensuring that a user's account is complete, correct, and acceptable.
- **Manual and Laborious Tasks**—The UAR procedures are error-prone, time consuming, and meticulous. A thorough examination of the user accesses within each team sometimes may take up to 4 weeks. Additionally, business leads have stringent deadline to complete a UAR. This time constraint may raise the likelihood of risks.
- **Review Frequency**—The best frequency to conduct UARs are quarterly and annually. But the lengthy and time-consuming nature of the process makes it challenging to conduct UAR every eight weeks. Bandwidth constraints cause delays that compound over time escalating organizational risks. A proper UAR executed on a regular basis can eliminate these hazards and result in operational efficiency.
- **Completeness and Accuracy**—UAR is frequently used as a catch-all by organizations who lack robust user administration function or role- and job-based accesses. However, it is critical for UAR owners devote adequate time to conduct thorough reviews.

Streamlining the UAR process

By restricting access to vital information and resources, user access review aims to lower security breaches and protect stakeholder trust. Having current access control regulations can make UARs quick, efficient, and simple. Below are three key themes that can help simplify user access procedures, promote compliance, and alleviate the pain points:

- **Defined Ownership**
  - User reviews require active participation from role owners. It becomes challenging to certify access when managers delegate the user accesses before structuring roles. People managers must also provide insights with respect to what activities and business functions their team must fulfill as part of their routine work duties.
  - Both operational and IT support personnel should work together to address any targeted questions about user access.
  - Privilege access bring inherent risks and hence, calls for more scrutiny. Roles with privileged access include IT administrators, business support staff, and security managers, which give their holders significantly more power than regular users, including the ability to grant or revoke access, change the level of access, and reset credentials. Such authorized users necessitate elevated setup, configurations, and security-related access to perform their duties.
- **Process Optimization**
  - In order to contribute value, it is critical that the person conducting the review comprehends the material thoroughly. Setting expiration dates can help make the UAR process simple and low risk particularly during instances where excessive entitlements are temporarily granted to a backup delegate.
  - Monitoring login activity by analyzing the "Last Login Date" can enable business process owners to track user inactivity and decide whether or not application access is required.
  - The optimal intervals to conduct UARs are quarterly and annually. While quarterly reviews focus on user access, annual reviews examine the changes to roles and profiles over the course of a year. It can help identify access controls that should be terminated.

- Setting clear expectations for target completion dates and defining a recurring schedule for reporting to UAR owners are crucial. Implementing preventative controls into your user and role provisioning processes can allow URs serve as re-attestations—not clean-ups.

- **Technology Enablement**
  - With accelerated technology adoption, automation is key to minimize human error, eliminate manual tasks, and easily discern modifications to security access. Through automation it is possible to streamline human capital management—the transition of joiners, movers, and leavers such that changes made to a user's status in the organization's HCM system are subsequently propagated to and integrated with underlying applications.
  - By using an exemption-based reporting it is easy to detect any modifications or alterations to user/role configurations between UAR periods, which can save time and cut down redundancy.
  - To improve the accuracy and completeness of the user access review, third-party solutions, such as ServiceNow, Sailpoint, and Fastpath can be leveraged to automate and monitor the process.

Closing comments

The need to control who has access to what systems and data is more than just a matter of enterprise security-it's a compliance necessity as well. Conducting user account review periodically is critical for monitoring, managing, and auditing the user account lifecycle to prevent potential risk concerns. UAR shouldn't be the tool you use to clean up access once a year, instead, it should validate the appropriateness of the work you've been doing all year. By being able to control "who has access to what" from the initial access request approval process to the fulfilment of access on target systems, UARs enable organizations to improve their overall security posture and prevent inappropriate access from being granted

Contact us

Christian Leva
Managing Director,
Application Security and Controls
KPMG LLP
T: 214-840-2000
E: cleva@kpmg.com

Joe Franczkowski
Managing Director,
GRC Technology
KPMG LLP
T: 267-256-3242
E: jfranczkowski@kpmg.com

Brian Jensen
Managing Director,
GRC Technology
KPMG LLP
T: 817-946-9552
E: brianjensen@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia