

---

# Six Best Practices for Executing an Effective and Efficient User Access Review



# Contents

Best Practice 1: Address IT Decentralization .....	3
Best Practice 2: Ensure Data Integrity .....	4
Best Practice 3: Enhance Accuracy Through Automation .....	5
Best Practice 4: Establish Trust in Automated Tools .....	6
Best Practice 5: Thoughtfully Determine the Right Scope and Frequency .....	7
Best Practice 6: Proactively Educate and Involve Stakeholders .....	7
Idira Identity Governance and Administration .....	8
About Palo Alto Networks .....	9

## BEST PRACTICE 1:

# Address 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. Organization must make sure they have thorough and robust IT coverage.

## 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

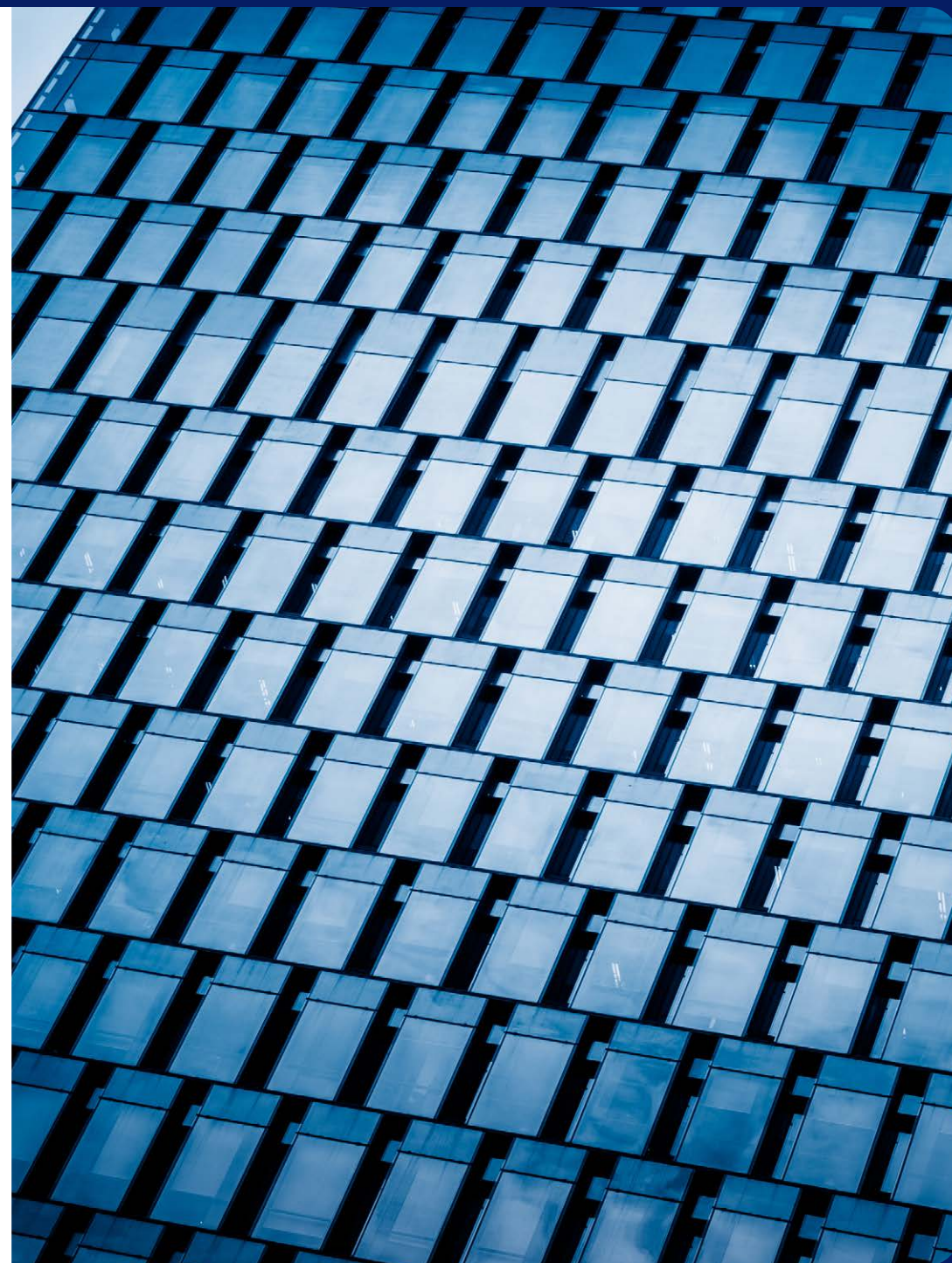
Use modern automation tools that integrate with a wide range of systems and platforms to help streamline the collection and analysis of data from disparate sources. Automation tools reduce the potential for human error and ensure that audit processes are both thorough and efficient.

## Simplify Audit Processes

Create and adopt nondisruptive audit processes that all departments can follow. They include developing easy and automated methods for data collection, standardized campaigns, and uniform criteria for collecting and evaluating the results. Ideally, your processes 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, 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:

# Ensure 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 both enhances the credibility of the data and 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:

# Enhance 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 susceptible to mistakes when performed manually. Many organizations struggle with this, as we can see from the 84% of organizations that rely heavily or entirely on manual processes.<sup>1</sup>

Automation streamlines User Access Review (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.

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. For example, we have taken a unique approach by using robotic process automation to retrieve 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.

1. *2025 State of IGA Survey Report*, CyberArk, July 2025.

## Campaign Readiness Stage

### Verifying Current Data

Conducting a thorough verification ensures that all applications, user accounts, and associated permissions included in the review are current. This step ensures 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 what they are approving or revoking.

### Correcting the 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.

### Correcting Reviewer Assignment

The right reviewer must be assigned for each user or account and application. An automated tool can help both initially and as any reassignments are needed.

### Preparing Audit Evidence

This stage also involves preparing and compiling all necessary audit evidence to support the review process. It might include before and after screenshots of application settings, logs of the review process, documentation of compliance controls, or any other evidence required by auditors.



#### BEST PRACTICE 5:

## Thoughtfully Determine the Right Scope and Frequency

A UAR is part of a program to mitigate risks that arise over time from user oversights and escalating privileges for the sake of productivity, resulting in a fundamental cost/benefit trade-off. 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.

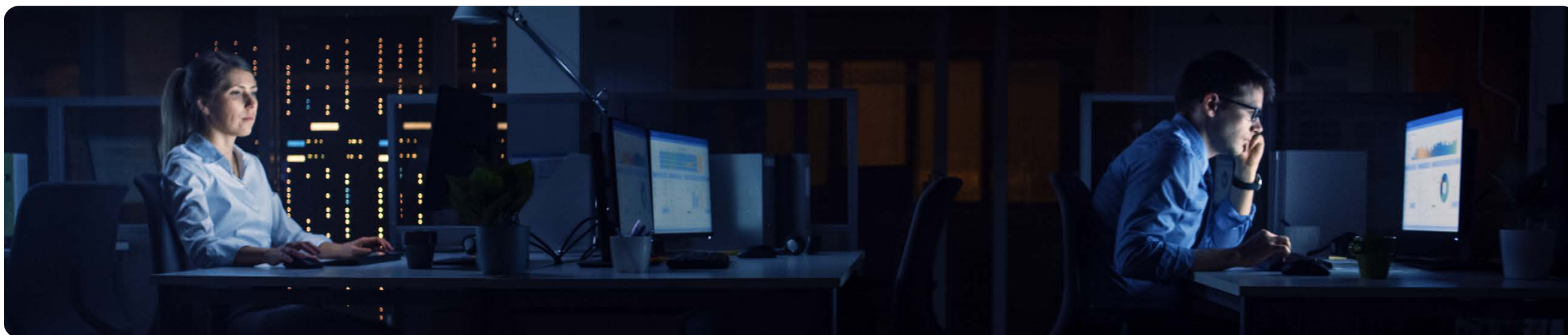
Leveraging automation is a significant benefit in meeting and exceeding the required frequencies of your UARs.

#### BEST PRACTICE 6:

## Proactively Educate and Involve Stakeholders

Thoroughly educate all relevant stakeholders about any new user access review processes or tools. This fosters trust and reliability from the outset. Internally, it might mean coordinating with internal audit teams, IT compliance teams, and application owners. Externally, it often 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.



# Idira Identity Governance and Administration

Idira™ Identity Governance and Administration, by Palo Alto Networks, 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 universal synchronization..
- 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-privileged 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, and application changes or revocations with screenshots.

To learn more about Idira Identity Governance and Administration, visit <http://www.paloaltonetworks.com/idora/identity-governance>.



# About Palo Alto Networks

Palo Alto Networks (NASDAQ: PANW), the global AI cybersecurity leader, protects our digital way of life with a comprehensive portfolio of cybersecurity solutions and platforms across Network, Cloud, Security Operations, AI, and Identity. Trusted by more than 70,000 customers and powered by Unit 42<sup>®</sup> threat intelligence, our AI-driven platforms eliminate complexity, empowering enterprises to modernize with confidence and securing the speed of innovation. Explore the future of security at [www.paloaltonetworks.com](https://www.paloaltonetworks.com).



3000 Tannery Way  
Santa Clara, CA 95054

Main: +1.408.753.4000

Sales: +1.866.320.4788

Support: +1.866.898.9087

[www.paloaltonetworks.com](https://www.paloaltonetworks.com)

© 2026 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.  
idira\_eb\_six-best-practices-for-executing-an-effective-and-efficient-user-access-review\_041626