7 tips to modernize your identity governance program

Drive productivity. Enhance security. Manage complexity.

When it comes to scaling your Identity Governance and Administration (IGA), automation is your not-so-secret weapon. Choose a unified Identity and Access Management (IAM) and IGA solution to strengthen your company's security posture, ease administrative IT burdens, and improve user experiences for your employees. Here are seven tips for building a modern approach to identity governance.

Access requests

Tip #1

Accelerate access request processes with familiar tools

Without automation
Handling approvals through endless help desk tickets and scattered email chains. Outdated internal docs provide questionable information about who can access what, resulting in long-lived access.

With automation
Utilize familiar productivity tools to handle app requests (e.g. Slack, Teams). Integrate with ITSM, time-based access, and build workflows for efficient, automated approvals.

Why it matters
Your team shouldn't have to spend time manually approving simple, everyday access requests using a tangled web of ad hoc solutions. Consider weaving the approval process into tools your team already uses and connect your tech stack with streamlined workflows, eliminating the need for lengthy end-user training.

Access requests

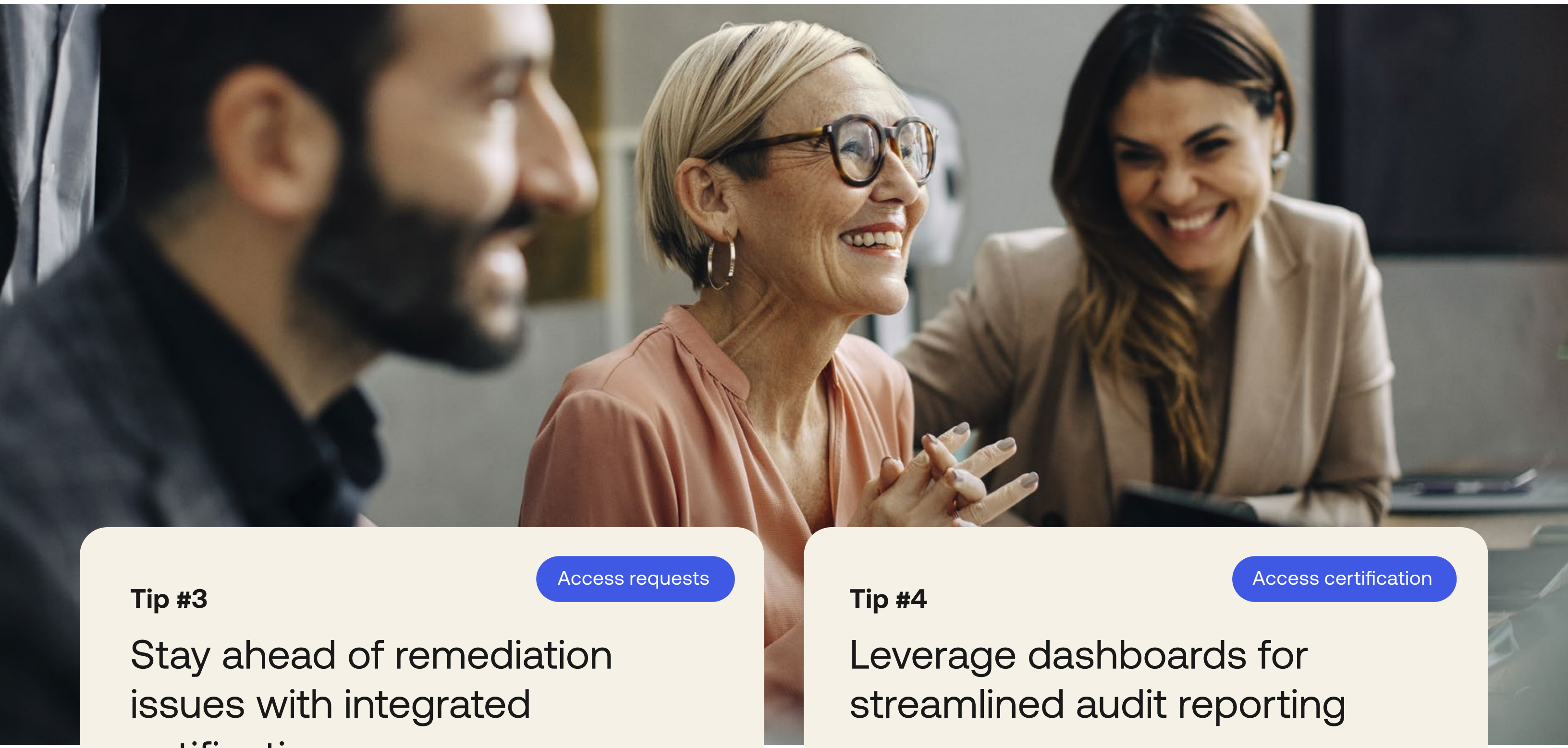
Tip #2

Convert app provisioning to group-based assignments

Without automation
Broad access to every app, regardless of team or role. This approach avoids friction, but it also creates an unnecessarily wide circle of access and scatters assignment duties across different teams.

With automation
Automate group-based app and policy-based entitlement assignments to keep access in the right hands. Maintain a unified source of truth by automating provisioning from external applications.

Why it matters
Automated provisioning and deprovisioning enable the right amount of access without creating a host of manual assignment tasks. Using group-based access assignments, IT teams can deliver access efficiently and peg assignment decision-making to a single, simple, automatically up-to-date source of truth.



Access requests

Tip #3

Stay ahead of remediation issues with integrated notifications

Without automation

If an employee's access is improperly disconnected, they don't find out until the moment they need to access mission-critical apps. Their remediation request is routed manually to whoever manages access to a particular app.

With automation

Leverage automatic notifications that alert users they've been disconnected and give them time to request access before it becomes an issue. Send automated approve/deny requests directly to your ITSM with familiar productivity tools like Slack or Teams.

Why it matters

Simple access issues sometimes turn into major UX problems, and slow, inefficient remediation can create deep frustration and productivity loss. Help employees stay ahead of this issue by remediating access issues with simple, fast approval requests.

Access certification

Tip #4

Leverage dashboards for streamlined audit reporting

Without automation

Chaotic spreadsheets and other manual efforts. These resources provide a (hopefully) up-to-date rundown of standing access profiles, albeit time-consuming and unintuitive.

With automation

Consult a centralized portal featuring access reports (complete with user-level details) that are automatically updated in real time. Use filters to get more detailed information relating to user access.

Why it matters

Audits can be complicated and painful—but they don't have to be. Level up your audits and boost understanding across teams using automation tools that assemble key information into compelling, digestible dashboards in seconds.

Access certification

Tip #5

Simplify certification campaigns with a centralized portal

Without automation

Lots of meetings with multiple teams to determine whether access should be validated or denied. The information from these meetings is stored in retrograde, insecure formats like spreadsheets and Word docs.

With automation

Define applications, entitlements, reviewers, managers, and remediation workflows in a central portal, giving IT a thorough portrait of access across the organization. Automate access approval/denial when required.

Why it matters

Similar to audits, certification campaigns can be inefficient and often lead to more clarity problems than they resolve. By centralizing access certification within an intuitive portal, IT can save time while restoring access decision-making to the proper channels.

Access certification

Tip #6

Unify governance policy with IAM

Without automation

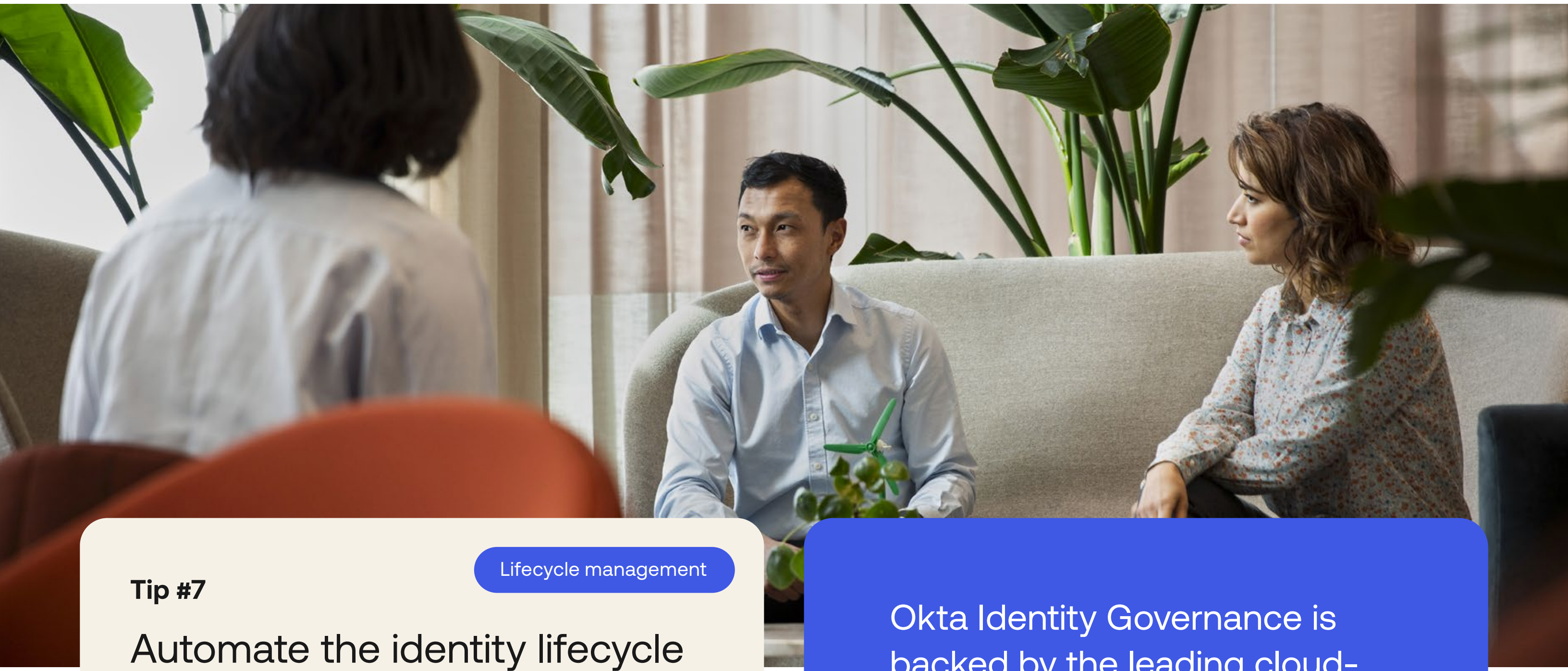
Different governance policies for different teams. Siloed policy regarding separation of duties and access certification leads to confusion and unnecessary friction, which leads to poor user experience and security gaps.

With automation

Unify IAM by centralizing identity governance, access management, and privileged access. Use governance policy to automate complex identity processes at scale.

Why it matters

Policy is only valuable insofar as it is understood across the organization and implemented in a consistent manner. The automated processes within unified IAM allow companies to scale confidently knowing that their governance policy can manage increasing volume.



Lifecycle management

Tip #7

Automate the identity lifecycle

Without automation
Individual app teams do their best to keep assignments up to date, but things inevitably slip through the cracks, allowing users to stay active in some apps after departing the organization.

With automation
Automate mover, leaver, and joiner processes so changes in user status are immediately reflected in apps. This way, HR-driven IT provisioning can keep up with changes in org structure and eliminate security gaps.

Why it matters
Automatic provisioning and deprovisioning are the key to a seamless, secure identity lifecycle. Embracing automation helps remove the prospect of human error, maintain the right levels of organization-wide access, and keep your workforce operating efficiently and securely.

Okta Identity Governance is backed by the leading cloud-based identity platform and can revolutionize the way your organization handles access requests, access certification, and lifecycle management. If you're ready to learn more about how Okta Identity Governance can help your organization scale quickly and securely, contact our team for a one-on-one demonstration.

Contact our team