Step-by-Step Guide:

How to Elevate Your Identity Lifecycle

okta

Table of Contents

A Journey Towards Visionary Lifecycle Management

All types of organizations struggle to keep up with the increasing pace of change in today's business environment, especially as remote workforces become more prevalent. At the same time, employee, partner, and customer expectations for frictionless—but still secure— experiences are soaring. Identity and access management platforms play a pivotal role in helping organizations address these demands by getting their end-to-end user lifecycle under control. With powerful automation, you can move from manual employee onboarding and offboarding IT tasks towards a modern approach.

In particular, the Okta Identity Cloud enables many forward-looking IT teams to streamline tedious provisioning, entitlement configuration, and deprovisioning processes. Many of our customers deploy Okta Lifecycle Management (LCM) to stay on top of identity changes via pre-integrated provisioning for 200+ apps, a universal directory with lifecycle awareness, and prescriptive lifecycle orchestration. This gives you the flexibility and agility you'll need to achieve visionary LCM workflows that not only decrease costs, but increase productivity and improve your security posture as well.

We've found that our most successful customers tend to incrementally modernize identity processes in a staged manner over time. In this way, you can quickly realize initial time savings and achieve fast ROI, rather than trying to configure every possible lifecycle management feature all at once. In this whitepaper, we'll provide a practical framework of best practices, recommendations, and goals for four common stages of lifecycle management maturity:

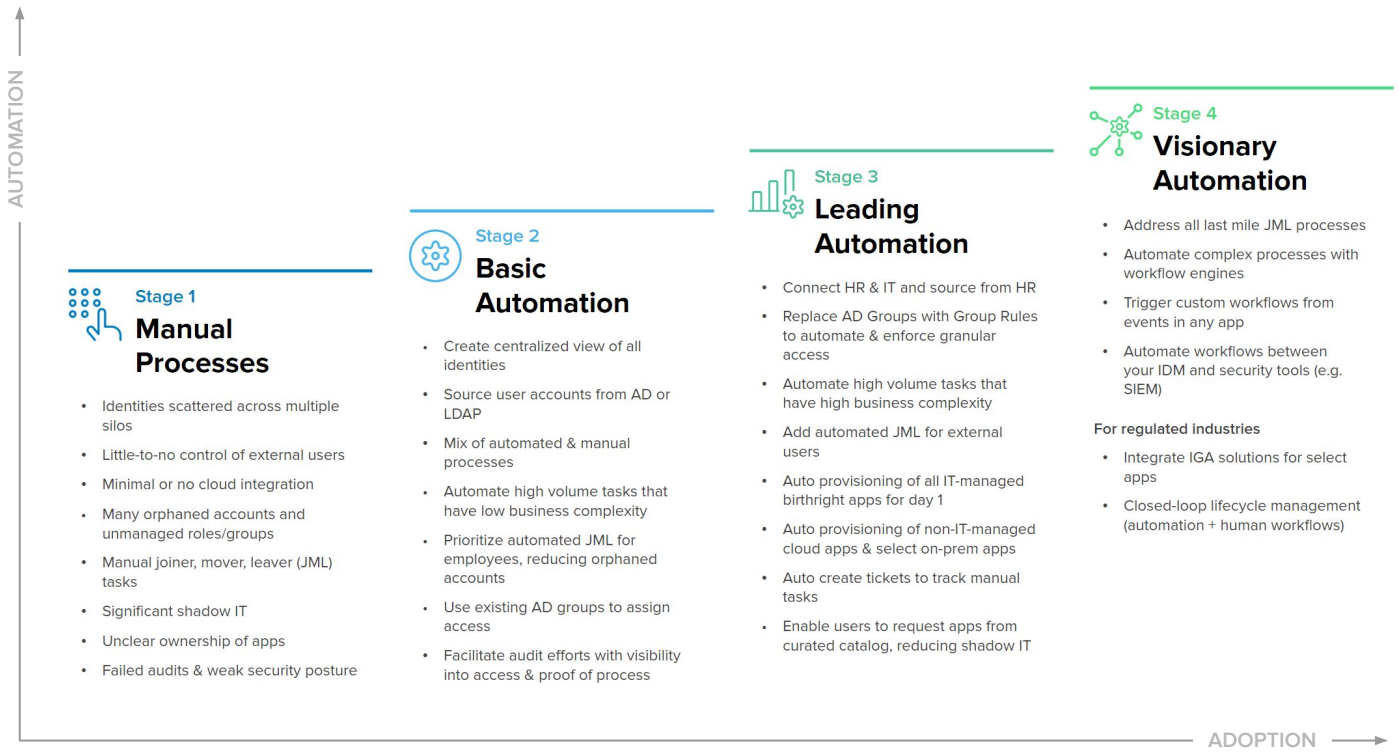

Figure 1: LCM Maturity Curve

Key Identity Lifecycle Challenges

Over the past decade-plus, Okta's experts have accumulated thousands of collective years of experience, lessons, and strategies from working with the 8,400+ organizations that rely on our platform as their foundation for identity and access management. Based on those insights, we developed the LCM maturity curve (fig. 1), along with the following detailed guidance. To help you tackle each phase at your own pace, the next section provides key prerequisites and gradual steps you should consider as you advance your approach to automation.

But first, it's important to understand that no matter how mature your identity strategy is, there are four primary areas of LCM that often confound IT and security teams: managing identity data, identity lifecycle processes, access grants, and audits and compliance.

Managing Identity Data

Managing identity data is all about creating a reliable system of record of all users—primarily your employees, but also contractors, partners, and customers. As such, it's usually the very first challenge teams face when they kick off a modern identity management initiative. Deploying any identity-related technology, such as single sign-on (SSO), provisioning, or multi-factor authentication (MFA), requires you to establish a single view of all the end users that access your IT ecosystem.

Creating this single view is difficult because it's fraught with questions like:

- What is my authoritative source of user information?
- If I have multiple sources, how do I synchronize data between them?
- How should I create unique usernames and email addresses?

Managing Identity Lifecycle Processes

More and more, we're noticing that identity lifecycle decision-making is no longer contained solely within IT. Increasingly, app owners and business unit managers determine who gets access. In addition, many organizations have implemented highly-customized business logic that most solutions can't handle out-of-the-box. Consequently, IT teams are frequently weighed down by at least some manual identity tasks.

Managing Access Grants

IT and security teams have the opportunity to offload tedious work by not only automating access decisions, but enabling self-service for end users as well. This reduces dependence on IT, and sets you up to securely and consistently grant access as your organization grows. However, it's becoming more difficult as remote work environments drive up demand for new digital collaboration resources, as well as temporary grants for elevated access.

Most likely, your access management strategy has to accommodate the following business requirements:

- Give people a variety of resources (applications, entitlements, roles, groups)
- Involve several stakeholders in access decisions (IT, business app owners, people managers)
- Meet individual needs through frequent exceptions (VIP accounts, parental leaves, alumni rehires)
- Take many confusing frameworks and models into account (attribute-based or role-based access controls, hierarchies, delegation)

Managing Audits & Compliance

Not to be overlooked, the fourth major challenge of effective identity management is managing audits and compliance. While your security team holds responsibility for helping auditors understand who has access to what, IT is often asked to provide that data for them. As you'd expect, the extent of this burden varies greatly across organizations. Some at the earliest stages of LCM maturity resort to long spreadsheets of account info—a time-consuming process. Others implement sophisticated identity governance and administration tools to automate access reviews.

Navigating the LCM Maturity Curve

Now that we've reviewed typical identity challenges, let's explore common scenarios, specific guidelines, and key benefits to expect as you progress through each stage of LCM maturity.

Stage 1

Manual Processes

Identity Data	Lifecycle Processes	Access Grants	Audits & Compliance
• Identities and credentials in multiple silos • Usernames or identifiers may not be globally unique • Identities constructed by hand	• Lifecycle process undocumented and administered manually • Poor logging, no accountability • Significant orphaned accounts present • Day-one access often delayed	• Proliferation of roles and groups with unknown purpose or owner • Lack of up-to-date core business role definitions • Users miss significant access on day one, resulting in high ticket volumes • Significant shadow IT	• Basic questions on who has access to what require significant investigation and time • No visibility of accounts created in the shadows - many unknown unknowns • Failed audits

Stage 1 recommendations for managing identity data

- Sync your existing directories into a single virtual view in order to centralize control over all your identity data. Be sure to:
  - Connect multiple silos like AD and LDAP into Okta Universal Directory (UD).
  - Include all users, but prioritize your largest population first (most likely employees).
  - *Pro tip*: Avoid domain consolidation, which is a long, costly undertaking.
- Choose the primary data sources and attributes you'll use to construct unique usernames.
  - For Okta usernames, configure formats for each data source.
  - For application usernames, ensure the desired attributes are imported to UD.
- Choose which data sources and data (attributes or groups) will be used to assign user access to various resources, and import it to UD.

During the initial stage of LCM maturity, IT teams handle provisioning and deprovisioning processes manually and waste considerable time on low-value joiner/mover/leaver (JML) "button pushing" tasks.

This is partly because user lifecycle events like hiring aren't coordinated with IT account creation. As a result, new hires rarely get timely access on their first day of work, and terminated users retain access for too long, creating security risks. If your organization is in this boat, you most likely have minimal documentation or accountability.

Stage 1 recommendations for managing identity lifecycle processes

- Take stock of all your current apps and their ownership.
- Survey your team to find out which apps involve the heaviest lift for JML support.
    - Differentiate apps provisioned via simple "button pushing" from those that require complex business logic which needs to be untangled or re-engineered.
- Determine whether a major app purchase (e.g. Office 365) is on the horizon.
- Create a prioritized list of 5-10 target apps to provision through Okta LCM.
    - *Pro tip*: Include apps with significant JML task load and/or your highest risk apps in order to demonstrate rapid ROI.

If you're constantly putting out fires related to access grants, it's impossible to meet the expectation of day-one account readiness for new employees. At this stage, business roles are often poorly defined, not updated, or not followed, leading to incorrect or delayed access. Instead, you find yourself scrambling to create ad hoc roles and groups, which in turn creates a mess of objects whose purpose eventually gets forgotten. After day one, if users request additional resources that IT can't adequately provide, they tend to procure apps or tools on their own—perpetuating shadow IT.

Stage 1 recommendations for managing access grants

- Create a map of your IT-owned vs. line-of-business (LOB)-owned applications and resources.
    - Determine the main mechanism for granting coarse-grained access to these apps, such as attributes or AD groups.
    - If applicable, identify any existing mechanisms and attributes for granting elevated admin privileges (site admin, user admin), or other roles (contributor, editor) in various apps.
- Clean up your unused access control roles and groups.
    - Review all groups in IT-owned sources (AD) to determine which are widely used, and which are unused and can be removed.

Each area of identity management influences how painful your audits are. In stage one, since the IT team is manually provisioning all your resources, you have no central record or logs. Additionally, widespread shadow IT means that every audit requires painstaking investigation, and failed audits are all too common.

Stage 1 recommendations for managing audits & compliance

- Understand what's in scope, including:
  - Which regulations is your company subject to? HIPAA, GDPR, CCPA, PCI?
  - What kind of data do you store (financial, PII), and which apps hold it?
- Understand the processes and data auditors look for in your organization, e.g.:
  - Employee offboarding
  - External user offboarding
  - Specific app access
  - Specific entitlements or admin access in certain apps
- Develop a systematic way to retrieve information, even if it's still manual for now.

Stage 2

Basic Automation

Identity Data	Lifecycle Processes	Access Grants	Audits & Compliance
• Single view of core user identity attributes (lifecycle state, groups, etc.) • Unique usernames and identifiers • Credential consolidation through federation, but minimal password sync	• Combination of automation and manual business processes for day-one access • Ad hoc handling of exceptions like VIP onboarding, hostile terminations, etc. • Fewer orphaned accounts	• Streamlined assignment of birthright access for IT-owned applications through core business roles • Additional access is the exception, medium ticket volumes • Some shadow IT, but most application owners are known	• Leveraging IdPs and directories to aggregate and view user access states as needed • Audit scope reduced thanks to better use of roles, policies, and automations • Majority of access grants run through auditable methods

At the second stage of LCM maturity, IT teams are just starting to implement automation, and still rely on many manual processes. If you're in this camp, automating account creation and updates from your IT-owned system of record is a great way to get a quick IT win, as it doesn't require lengthy coordination with other departments. As you automate provisioning or deprovisioning for birthright apps that all employees need, like email and storage, you'll accelerate your time-to-value.

Stage 2 recommendations for managing identity data

- Source user profiles and unique identifiers from all of your authoritative IT directories (AD or LDAP), and pull them into Okta UD.
- Establish centralized control and one view of all user accounts, regardless of where they reside (in LDAP 1, LDAP 2, AD domain 1, AD domain 2).
- Manage your groups, credentials, and lifecycle states in AD/LDAP and configure Okta to regularly import these changes into UD.

Stage 2 recommendations for managing identity lifecycle processes

- Use triggers from IT sources (a new user, updated user, or terminated user) to drive provisioning or deprovisioning actions in Okta (create or remove an account in Okta, Box, Office 365).
- Fully configure your first app for automated on/offboarding
    - Maximize ROI by choosing an app with the highest volume of JML tasks and lowest business logic complexity.
    - Autoprovision at least two IT-owned, birthright apps for day-one access.
    - *Pro tip*: Consider enabling account provisioning for IT-owned, birthright apps to boost productivity, or enabling broad account deactivation to boost security.
- Prioritize automated JML for employees, which will reduce orphaned accounts.

As you get a better picture of your access grant landscape, your IT team can shift gears towards working with other departments to define (or redefine) their core business role definitions. IT then uses roles to systematically grant access with rigor, improving the organization's security posture. Users will value the IT team and request additional access by following prescribed practices, reducing Shadow IT. In stage two, IT can facilitate audits by providing lists of users, groups, and associated roles.

Stage 2 recommendations for managing access grants

- Establish your business role definitions using clear naming conventions in collaboration with key LOB app owners.
- Map these business roles to your IT access control groups (AD groups).
    - *Pro tip*: Set up Okta's group rules with data from your IT sources of truth for flexible, future-proof maintenance.
- Use AD/LDAP groups to assign birthright access to your IT-owned apps, including:
    - Coarse-grained access (assignment to the app itself)
    - Fine-grained access (assignment to specific entitlements within the app)

Stage 2 recommendations for managing audits & compliance

- Create handy playbooks that document how to pull users, entitlements, accounts, and access log data for audits.
    - *Pro tip*: Leverage your identity platform and directories (users, groups, roles) to ensure accurate reporting.
- Show proof of your onboarding and offboarding processes from IT sources of truth.

Stage 3

Leading Automation

Identity Data	Lifecycle Processes	Access Grants	Audits & Compliance
• Identity data (especially data used for access logic and policies) automatically pulled from sources of truth • Self-service credential management	• Prompt, consistent, comprehensive day-one access • Full onboarding through multi-stage automation, including credential setup • Automation for detailed business requirements like timezone-based activation • No orphaned accounts	• Finer-grained user- or application-level entitlements handled in coordination with LOB and app owners • Streamlined self-service means IT is not bottleneck between users and app owners	• Generating continuous reports and analytics on who has access to what • Optimizing for more than audits; data starting to drive proactive risk mitigation and cost control

In the next phase, leading IT teams integrate their identity data (email address and phone numbers) with HR sources (personnel data and lifecycle events like hiring and terminating), enabling deeper automation that benefits from faster lifecycle signals. These best practices can power more nuanced identity workflows, such as changing access grants due to parental leave, staging accounts before an employee's start date, granting alumni access to specific resources, and automating leaver processes for both employees and external users.

Stage 3 recommendations for managing identity data

- Transition to sourcing user profiles and lifecycle states from your HR system, with data constantly flowing from HR to Okta, and from there to other downstream IT resources, including directories.
- Configure a bi-directional sync of user attributes as needed.

- Automatically source identity data (especially data used for access logic and policies) from various departments.
- Replace manually managed AD/LDAP groups with Okta's group rules, and start using data from both HR and other IT apps to automatically set group memberships.

Stage 3 recommendations for managing identity lifecycle processes

- Source identity profiles from your HR system and trigger workflows off of lifecycle changes in your HR system.
    - *Pro tip*: Fully automate day-one access and terminations for employees.
- Eliminate orphaned accounts. The two main steps to do so are:
    - For employees, trigger the leaver process from your HR signals.
    - For external users (who are typically not in HR systems), automate the leaver process with preset policies (e.g., suspend after X days of inactivity).
- Automate deprovisioning for your highest-risk applications, including:
    - Internet-facing applications (public cloud apps or homegrown apps running in the cloud);
    - Critical internal systems that store PII data, like your payroll system
    - Any apps containing sensitive customer data, such as your CRM, ERP or analytics platforms.

All of these LCM strategies deliver substantial productivity improvements, empower LOB stakeholders, and extend self-service for end users so they can get appropriate apps without IT intervention. You'll have reliable onboarding and offboarding processes in place for all user types, which helps with audits. And by elevating the efficacy of your audit efforts, you'll reduce both risks and costs.

Stage 3 recommendations for managing access grants

- Replace manually managed groups with automatically managed ones to streamline birthright access assignments.
    - Use Okta's group rules to instantly put users into (or take them out of) groups based on attribute changes.
    - *Pro tip*: Be sure to base access grants on attributes (department and/or location) as much as possible, using existing AD groups ("enterprise sales") only when necessary.
    - Use HR data (contact information or job-specific data like titles, manager) and IT data (user ID, email address, entitlements) to assign access.
- Coordinate more closely with LOB app owners and help them set fine-grained entitlements for users of function-specific apps, such as CRM or marketing systems.
    - *Pro tip*: For requests with sufficient identity data, route access requests directly to LOB owners via automated ticket creation and alerts that include IT user data.
    - Delegate simple resource assignment decisions to application owners.

- Implement self-service for end users to scale high-volume, low-risk access requests.
    - Delegate access approvals out of IT where possible, while ensuring appropriate approvals and oversight.

Stage 3 recommendations for managing audits & compliance

- Facilitate audits with Okta's out-of-the-box reports.
    - Use the Current Assignments report to show all current access grants to each cloud app.
    - Use the Recent Unassignments report to check deprovisioned access records.
- Facilitate audits by documenting and providing proof of your process.
    - For employees, show how you on/offboard from your HR systems.
    - For external users, show your policy-based offboarding process.
- If needed, make this data available to your third-party visualization or analytics tools like Tableau, Snowflake, and Splunk.
    - *Pro tip*: Implement real-time analytics on multiple access slices for more granular visibility (by user, by resources, by time).
- Implement proactive risk mitigation and cost control. For example, you can use:
    - Lifecycle triggers to alert third-party systems or run complex workflows, such as killing sessions or suspending accounts after a specified time period; or
    - Lifecycle triggers to revoke or downgrade app licenses.

Stage 4

Leading Automation

Identity Data	Lifecycle Processes	Access Grants	Audits & Compliance
• End users provide their own data (establishing usernames, name changes) • Access to dynamic identity data (teams, projects, PTO) • IT as a service to the business, supplying identity data and roles	• Exceptions like rehires or role changes handled with structured workflows • Even complex identity lifecycles automated (heavy business process, users of multiple user types) • IT provides tools for LOBs to self-manage complex processes	• After access is granted, it is consistently pruned • Additional factors feed into access decisions, like security risk, cost, usage, projects, etc. • Self-service expands, allowing LOBs to manage their own applications, roles	• Intelligence and analytics provide key insights • Using data to power better user experiences and end-user productivity

Finally, IT teams that fully optimize their identity processes and aggregate all required data are freed up to better serve the needs of other departments, perhaps by automating certain LOB or geo-specific tasks or by enabling them to build workflows themselves. As a result, you can better adapt to evolving workplace dynamics—rehires, role changes, remote and contract work—that require more complex, but flexible, approaches, like time-based or project-based access. In the visionary automation stage, you'll see the most efficiency gains from automating these intricate processes.

Stage 4 recommendations for managing identity data

- Find opportunities for end users or line of business admins to update data.
- Identify cross-organizational needs for identity data, and automate sharing between relevant systems.
- Determine whether it's feasible to ingest dynamic identity data—such as teams, projects, PTO—into Okta UD, and use it to set granular, temporary, or elevated access.

Stage 4 recommendations for managing identity lifecycle processes

- Leverage the no-code Okta Workflows automation platform for your complex IT processes.
    - If necessary, build bespoke JML processes to perfectly fit your organization's needs, e.g. a college student who simultaneously becomes a teaching assistant (faculty) and later an alumnus, or a contractor who becomes a full-time employee of an organization.
    - *Pro tip*: Use easy-to-build workflows to perform deep, granular actions in your apps (such as setting default folder shares in Box when provisioning accounts).
- Auto-create tickets in your ITSM system (e.g. ServiceNow) to nudge admins to take action on the few manual tasks remaining (creating an account in a custom-built or legacy app)
    - Populate the ticket with identity data.
    - *Pro tip*: Tie the update or closing of a ticket with your identity system (enable SSO to the manually provisioned legacy app and log the transaction).
- Enable other departments to create automated workflows, for example:
    - Security team regularly extracting identity data for audits
    - Security team setting up live notifications for suspicious identity-related activity
    - Salesforce admins automating complex assignment of entitlements

Organizations with a visionary approach to granting access will see the greatest improvement to their security posture by incorporating additional insights into access decisions and systematically pruning and purging not just orphaned accounts, but all stale roles, entitlements, and groups. At this level of LCM maturity, LOB stakeholders can benefit from shared identity data to manage their own applications and roles.

Stage 4 recommendations for managing access grants

- Devise a continuous authorization strategy to support Zero Trust.
    - Implement time-bound, contextual access parameters for resources (looking at security risk, cost, usage, projects).
    - *Pro tip*: Configure periodic reauthorizations to maintain clean access policies.
- Regularly review all access control groups and entitlements.
    - Be proactive by setting up automatic alerts for unused resources.
- Delegate more complex resource assignment decisions to application owners.
    - *Pro tip*: Kickstart the process by creating baseline accounts for key LOB stakeholders.
    - Pass identity attributes, roles, and groups data to app owners via IT tickets, automated emails, Slack messages, or perhaps a shared spreadsheet.

Stage 4 recommendations for managing audits & compliance

- Use Okta APIs to retrieve data for audits.
- Give your end users, managers, and application owners visibility into the current state of access, with the opportunity to flag access anomalies.
- Create real-time alerts or audit logs for high-risk, high-value access changes (new privileged accounts, entitlement step-up).
- *Pro tip*: For regulated industries that require significant governance, you may want to integrate Okta with an IGA solution like SailPoint or Saviynt at this stage. An integration with Okta will provide the IGA solution with rich identity data (users, app assignments, groups, roles, entitlements) and a mechanism to remediate access to apps managed by Okta.

Increasing IT Agility with Identity Automation

Each organization has its own unique lifecycle requirements and priorities, so you should adapt our identity recommendations to the strategies and techniques that best fit your needs. No matter how you deploy Okta's end-to-end suite for modern identity management, you'll be able to ensure day-one access for employees and prevent former users from retaining business accounts—improving productivity and enhancing security.

In particular, Okta's cloud-based identity and access management solution removes roadblocks to onboarding and offboarding by integrating employee information from IT systems (including Active Directory), as well as the most popular HR applications (Workday, SuccessFactors, UltiPro, BambooHR, and Namely). With Okta's Universal Directory, organizations can centralize accounts from all of these data stores and establish one identifier per employee. Okta Lifecycle Management (LCM) enables IT teams to simply click a checkbox and orchestrate repetitive identity tasks, such as creating, updating, or deactivating accounts, configuring policies, and reporting on access levels across your ever-shifting workforce and their devices. To learn more, visit okta.com/products/lifecycle-management.

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 8,400 organizations, including JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to help protect the identities of their workforces and customers

www.okta.com