ConductorOne

Understanding the Key Phases of Identity Lifecycle Management

Identity lifecycle management (ILM) is the comprehensive process of managing digital identities for users throughout their lifecycle within an organization. This includes:

- → Creating new identities for new users (employees, contractors, guests) and granting them appropriate access to resources.
- → Updating existing identities as roles and responsibilities change, ensuring users have the correct access privileges.
- → Monitoring access levels to prevent security risks and ensure compliance with policies.
- → Offboarding users by revoking access and deprovisioning identities when they leave the organization.

Essentially, ILM is about ensuring the right people have the right access to the right resources at the right time.

Why is identity lifecycle management important?

Organizations face increasing challenges in managing user identities and access. Traditional approaches often rely on inefficient manual processes, leading to security vulnerabilities and operational bottlenecks. This can result in:

→ **Delayed onboarding**: New hires waiting days or even weeks for access to essential resources, hindering productivity.

→ **Stale accounts and privileges**: Former employees or those who have changed roles retaining unnecessary access, increasing security risks.

→ **Errors and inconsistencies**: Manual processes are prone to human error, leading to incorrect permissions, unauthorized access, and potential security gaps.

ILM solutions can address these challenges and automate critical tasks, ensuring:

→ **Rapid onboarding**: New employees gain access to the resources they need quickly and efficiently.

→ **Proper deprovisioning**: User accounts and access are revoked promptly when employees leave or change roles.

→ **Accurate and consistent access**: Automated processes reduce errors and ensure that users have the correct permissions based on their roles and responsibilities.

Beyond access management, ILM processes help mitigate security risks by:

→ **Detecting and preventing insider threats**: ILM helps prevent disgruntled employees or malicious actors from exploiting dormant accounts or excessive privileges.

→ **Preventing privilege creep**: By regularly reviewing and updating user access, ILM helps eliminate the accumulation of unnecessary permissions over time.

→ **Enhancing security posture**: Strong authentication, access controls, and activity monitoring strengthen the overall security posture of the organization.

These benefits also help to:

→ **Empower employees**: Self-service features allow users to manage their own accounts and access, reducing reliance on IT support.

→ **Optimize IT resources**: Automation frees up IT staff to focus on strategic initiatives rather than tedious manual tasks.

→ **Support business agility**: ILM enables organizations to quickly adapt to changes in workforce, roles, and responsibilities.

Identity lifecycle management phases

Identity creation

Before an individual can interact with any systems, their digital identity needs to exist. This often involves:

- **Collecting core information**: Name, employee ID, department, role, etc.
- **Establishing initial access**: What systems and resources do they need on day one? This should align with the principle of least privilege.
- **Setting up authentication**: Creating their login credentials, potentially including multi-factor authentication (MFA) or biometrics for enhanced security.

Automation is key: Ideally, much of this is automated through HR systems or identity management platforms to reduce manual effort and errors.

Onboarding and user provisioning

This phase bridges the gap between identity creation and active participation in the organization's digital environment. It's about smoothly integrating the new employee's identity into identity and access management (IAM) systems and ensuring they have the right access from day one.

Onboarding can be conducted with or without modern IAM systems. Let's take a look at the difference:

Onboarding with modern IAM systems

- When HR systems and identity platforms (IdPs) are integrated, the process becomes significantly easier. The identity created in the HR system (like Workday or BambooHR) is automatically synced with the IdP (like Entra AD or Okta).
- The employee's role in the HR system dictates their access privileges. This is often managed through groups in the IdP, where each group has predefined access to specific resources. This automation ensures consistency and reduces errors.

Onboarding without IAM tools

- Without integration, the process becomes heavily reliant on manual coordination between HR and IT. This increases the risk of errors, delays, and inconsistencies.
- Manually providing access permissions can lead to overprovisioning (granting excessive access) or underprovisioning (restricting necessary access). Both can negatively impact productivity and security.
- IT staff have to manually create accounts, assign permissions, and ensure compliance with the principle of least privilege, which can be a significant burden, especially with multiple new hires.

The other primary identity lifecycle management task that needs to happen during onboarding is email creation. A new employee's email address is a key component of their digital identity. It needs to adhere to organizational standards and be created promptly to facilitate access to resources and communication.

Monitoring, reporting, and maintenance

This is the ongoing phase of ILM focused on continuous oversight and optimization. It's about ensuring that identities and access remain appropriate, secure, and compliant over time. Think of it as the continuous care and upkeep of your identity management system.

Several key tasks are involved:

Access monitoring

Continuously track who has access to what resources and why. This allows you to:

- → **Identify and respond to suspicious activity**: Detect potential security breaches or insider threats.
- → **Prevent privilege creep**: Spot and rectify situations where users have accumulated more access than they need.
- → **Ensure least privilege access**: Verify that users have only the necessary permissions to perform their job duties.

Reporting

Generate reports on user access and permissions to:

- → **Demonstrate compliance**: Prove adherence to regulations and internal policies.
- → **Support audits**: Provide evidence of access controls and security measures.
- → **Gain insights into access patterns**: Identify trends and potential risks.

Access maintenance

Maintaining appropriate user access throughout the identity lifecycle is essential. As users change roles, join new teams, or take on additional responsibilities, their access should be regularly reviewed and updated. This includes:

- → **Modifying permissions**: Granting or revoking access to applications, systems, and data as needed.
- → **Updating user attributes**: Keeping information like job titles and department affiliations current.
- → **Managing group membership**s: Adding or removing users from groups to efficiently manage access.
- → **Preventing privilege creep**: Ensuring that users don't accumulate excessive access privileges over time, which poses a significant security risk.

A centralized identity governance and administration (IGA) tool simplifies the monitoring, reporting, and maintenance phase of ILM. By consolidating access decisions, approvals, and monitoring into a single platform, IGA solutions provide security teams with the control and insight needed to govern access effectively.

Offboarding and user deprovisioning

This is the final and one of the most critical phases of ILM. It's about ensuring that when someone leaves the organization, their access to systems and data is revoked promptly and completely to prevent security risks. Think of it as the "exit procedure" for digital identities.

Secure offboarding is vital to:

- → **Mitigate threats**: Ex-employees who retain access, even unintentionally, pose a significant security threat. They could potentially access sensitive information, disrupt operations, or cause reputational damage.
- → **Minimize the window of vulnerability**: IT must act quickly to revoke access and deprovision identities to minimize the window of vulnerability.

Similar to onboarding, the offboarding process can be conducted with or without modern identity management solutions. Let's take a look at the difference:

Offboarding with IAM tools

- → When HR and IAM systems are integrated, offboarding becomes much more efficient. The act of deactivating or deleting the employee's identity in the HR system automatically triggers the same action in the IAM system, revoking all associated access.
- → Even with automation, both HR and IT should perform final checks to ensure complete deprovisioning and prevent any oversight.

Offboarding without IAM tools

- → Without IAM tools, offboarding relies on manual coordination and communication between HR and IT, increasing the risk of delays and errors.
- → Delays in revoking access can leave the organization vulnerable to data breaches or other security incidents.
- → Manually deprovisioning accounts and revoking access across multiple systems is time-consuming and prone to errors, especially for IT teams already managing a heavy workload.

ILM for managing external and guest identities

Many organizations collaborate with external users like contractors, vendors, partners, or temporary staff. These individuals often need access to internal resources, making it essential to manage their identities effectively.

The core phases of ILM (creation, onboarding, monitoring, offboarding) still apply to external identities. However, there are some key differences:

- → **Temporary access**: External users typically require access for a limited duration or specific projects.
- → **Varying levels of access**: The level of access granted to external users will depend on their roles and responsibilities.
- → **Increased need for flexibility**: The lifecycle of external identities is often more dynamic, with frequent changes in access needs and durations.

Additionally, the ability to suspend an identity is crucial for managing external users. Suspension temporarily revokes all access without permanently deleting the identity. This is useful for:

- **Temporary departures**: When a contractor's project is on hold, their identity can be suspended and quickly reactivated when needed.
- **Seasonal workers**: Identities can be suspended during the off-season and reactivated when they return.
- **Access reviews**: Suspending an identity during an access review allows for a thorough evaluation without completely removing access.

ConductorOne

Streamline identity lifecycle management with ConductorOne

ConductorOne is purpose-built to automate and simplify identity lifecycle management (ILM). It focuses on helping organizations manage user access and permissions across various applications and systems, ultimately making ILM more efficient and secure.

Here's how ConductorOne can assist with ILM:

Automated user onboarding and offboarding

- **Streamlined provisioning**: ConductorOne automates the creation of user accounts and granting of access privileges across different applications, reducing manual effort and ensuring consistency.
- **Simplified deprovisioning**: When an employee leaves or changes roles, ConductorOne can automatically revoke access to applications and systems, preventing security risks associated with stale accounts.

Centralized management of user access

- **Unified view**: ConductorOne provides a single dashboard to manage user access across all applications, giving administrators a clear overview of permissions and entitlements.
- **Delegated administration**: It allows for the delegation of access management tasks to different teams or individuals, improving efficiency and control.

Enforcement of least privilege access

- Policies defining role- and attribute-based access control can be enforced dynamically, ensuring access is adjusted when users' access needs change.
- Just-in-time provisioning: ConductorOne can grant access to resources for a limited amount of time, further minimizing the risk of unauthorized access.

Integration with existing systems

→ **Wide range of connectors**: ConductorOne integrates with a wide variety of IdPs, HR systems, and cloud and on-prem applications and infrastructure, including homegrown systems, enabling seamless ILM across the organization's IT ecosystem.

→ **API-driven approach**: Its API-first approach allows for customization and integration with other tools and workflows.

Enhanced security and compliance

→ **Automated access reviews and reporting**: ConductorOne facilitates regular access reviews, ensuring that users have only the necessary permissions for their roles, and auditor-ready certification reports are easily generated at any time.

→ **Audit trails**: It provides detailed audit logs of all user access changes, supporting compliance with regulatory requirements.

Why customers choose ConductorOne for ILM

Legacy identity systems are slow, complex, and often leave gaps in security and compliance. ConductorOne was built to change that. Customers choose ConductorOne because it delivers immediate, measurable improvements to their identity lifecycle processes—automating the hard parts, reducing operational overhead, and strengthening security across the board.

From fast onboarding and precise deprovisioning to real-time visibility and policy enforcement, ConductorOne gives teams the tools they need to manage access with confidence—and without compromise. Here's how customers are seeing real results with our platform:

instacart

Improved security: ConductorOne reduces the risk of data breaches and insider threats by enforcing least privilege access and automating deprovisioning. Companies like Instacart trust ConductorOne to eliminate standing access, detect overprovisioning, and enforce just-in-time access across their cloud infrastructure.

85%

Increased operational efficiency: Our platform streamlines user onboarding and offboarding, freeing up IT resources and improving productivity. ConductorOne customers also routinely report completing access reviews with 85% less effort than before.

SYSTEM

Reduced costs: Deployments are fast—typically within weeks, not months (or years). With ConductorOne, System1 onboarded key applications and launched a privileged access campaign in just three weeks.

RRCU

Enhanced compliance posture: We help organizations meet their compliance obligations with confidence through audit trails and access controls. After adopting ConductorOne for access governance, RRCU achieved a $1 million risk reduction and 2,000% ROI.

DigitalOcean

Improved user experience: Reviewers and end users complete tasks quickly and intuitively. DigitalOcean achieved a 100% on-time completion rate across seven departments by using ConductorOne's review UI.

Tired of inefficient processes and security risks associated with managing user access? Book a demo to see for yourself how ConductorOne can streamline your ILM processes.

Try ConductorOne now

Get a demo

ConductorOne

AICPA SOC