cerby

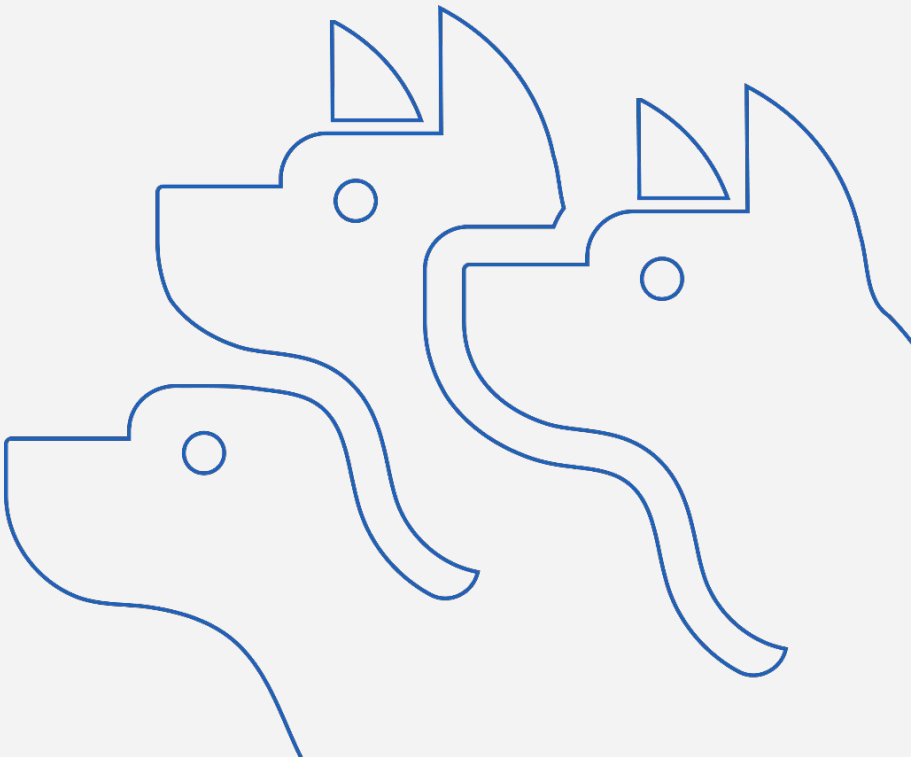
Audit Guide

# Identity Lifecycle Audit Guide

cerby

# Table of Contents





cerby

## Introduction

# Why this matters now

Most identity programs easily automate lifecycle management for connected apps, but cannot do the same for business-critical tools that don't have APIs or support SAML or SCIM. Social platforms, HR tools, finance portals, and on-prem systems are just some of these blind spots, forcing teams to rely on manual provisioning, shared credentials, and delayed access changes.

**>80%**

of hacking-related breaches are linked to weak or compromised credentials

source

**85%**

of infrastructure attacks could be mitigated by basic access management security

source

**47%**

of organizations failed to meet regulatory compliance regulations due to the inability to secure disconnected applications

source

# How to use this checklist

This audit guide focuses on identity lifecycle controls (provisioning, access changes, and deprovisioning) commonly assessed in SOC 2, ISO 27001, and SOX audits. Use this guide to assess how well identity lifecycle controls work across disconnected apps, identify your highest-risk gaps, and determine whether your approach will hold up under audit scrutiny.For each question, mark **Yes** / **No** / **Partial** based on your current state:

- Flag any **No** or **Partial** responses, these are control gaps.
- **Count the red flags**, 4+ responses indicate a higher risk environment.
- **Note manual dependencies**, these are the biggest vulnerabilities

cerby

SECTION 1

# Do you have visibility & ownership?

You can't govern what you don't see. Disconnected apps lack integration with identity tooling and sit outside IT oversight, hiding blind spots and security risks.

## Inventory & scope

- [ ] Do you have a current inventory of all apps, including those managed by business teams without IT oversight (social platforms, HR tools, finance portals, on-prem systems)?
- [ ] Does this inventory identify which apps don't support SSO or SCIM?

---

## Ownership & accountability

- [ ] Is there a documented owner for each disconnected app?
- [ ] Is ownership tied to a role (not just a person's name)?
- [ ] Do owners know they're responsible for access approvals and removals?
- [ ] Do owners have defined SLAs for approving/revoking access?

---

## Red flags 🚩

- [ ] Only apps in your IdP are tracked
- [ ] App owned by someone who has left or changed roles
- [ ] Accounts tied to personal emails or former employees
- [ ] No expectations or accountability regarding SLAs for access changes

cerby

SECTION 2

# Can you prove lifecycle control?

Access risk builds across the identity lifecycle. It starts when disconnected apps are excluded, grows when role changes don't update access, and peaks at offboarding when deprovisioning is delayed and credentials aren't rotated.

## Provisioning

- [ ] Are baseline (“birthright”) apps clearly defined for all employees?
- [ ] Are department- or role-based apps provisioned automatically?
- [ ] Is birthright access assigned based on role, department, or group, not individual decisions?
- [ ] Does provisioning work for disconnected apps, not just SSO-enabled ones?
- [ ] Can new hires access required disconnected apps on their first day?

---

## Access requests

- [ ] Is access requested through a formal, trackable process?
- [ ] Are approvals required for non-birthright access?
- [ ] Can business owners approve access without IT manually logging into each app?
- [ ] Is there a clear record of who approved access and when?

---

## Least privilege & security hygiene

- [ ] Are users granted only the access required for their role?
- [ ] Are shared or admin-level permissions restricted and time-bound?
- [ ] Are credentials created and stored centrally (never sent to users via email or DM)?
- [ ] Is MFA enforced by default, including for shared or legacy apps?

cerby

## Deprovisioning & offboarding

- [ ] Is access to disconnected apps revoked immediately when a user leaves?
- [ ] Is deprovisioning triggered automatically by HR or IdP events?
- [ ] Are orphaned accounts automatically detected and disabled or reassigned?
- [ ] Are shared credentials rotated automatically when users depart?
- [ ] Is external access (vendors, agencies, contractors) time-bound by default and automatically expired?

---

## Red flags 🚩

- [ ] Access requests happen informally
- [ ] Birthright access is inconsistent across users in the same role
- [ ] Everyone has the same permission level in critical apps
- [ ] Passwords shared via email, Slack, or spreadsheet
- [ ] No clear record of who approved access and when
- [ ] Deprovisioning takes 1+ days after termination
- [ ] IT must manually log into each app to remove access
- [ ] Former contractors or agencies still have active access
- [ ] Shared passwords unchanged after employee departures

cerby

SECTION 3

# Can you survive an audit?

If you can't prove it, auditors assume it didn't happen.
Disconnected apps often lack centralized visibility, making audits slow, manual, and error-prone.

## Reporting & access reviews

- [ ] Can you easily produce a list of who has access to each disconnected app?
- [ ] Can you show when access was granted, changed, or revoked?
- [ ] Are disconnected apps included in regular access reviews and certifications?

---

## Logging & accountability

- [ ] Is user activity tied to individual identities, even for shared accounts?
- [ ] Are access changes logged and retained for compliance purposes?
- [ ] Can logs be exported to your SIEM or GRC tools?

---

## Red flags 🚩

- [ ] Access reports assembled manually in spreadsheets before audits
- [ ] No audit trail for access changes
- [ ] Shared logins with no attribution to individuals

cerby

SECTION 4

# Is your approach scalable?

Manual processes don't scale and brittle scripts eventually fail.
This section evaluates whether your current approach can survive growth, app changes, and turnover.

## Automation vs. manual work

- [ ] Do lifecycle workflows run without custom scripts or manual intervention?
- [ ] Do automations survive UI or workflow changes in the underlying apps?
- [ ] Is ongoing maintenance minimal and owned by a team, not one person?
- [ ] Can you onboard a new disconnected app in days, not months?

---

## Red flags 🚩

- [ ] Automations owned by one engineer who "knows how it works"
- [ ] Scripts that break when apps change and require constant fixes
- [ ] Manual steps required to complete provisioning or deprovisioning
- [ ] New disconnected apps added to "manual process" list by default

cerby

# Assess your risk

## Scoring

Based on **Yes** or **Partial** responses

- **0-3 gaps:** You're in good shape, focus on maintaining controls
- **4-8 gaps:** Moderate risk, prioritize automation and governance
- **9+ gaps:** High risk, you're exposed to audit failure and security incidents

## What good looks like

| Without Automation | With Automation |
|---|---|
| 3-5 days to provision access | Same-day access for new hires |
| Manual spreadsheet audits | Auto-generated compliance reports |
| Shared passwords in Slack | Centralized, auto-rotated credentials |
| Deprovisioning takes days or weeks | Immediate revocation on termination |
| Scripts break when apps change | Workflows adapt without maintenance |
| Orphaned accounts discovered manually | Continuous monitoring and auto-remediation |

## Ready to close these gaps?

If this audit revealed control gaps or manual dependencies, you're not alone — and you don't have to fix it with scripts and spreadsheets.

**Next steps:**

- ✓ **Share this audit** with your team
- ✓ Book a free assessment and get a personalized gap analysis
- ✓ See how Cerby works and learn how Cerby automates disconnected app lifecycle management