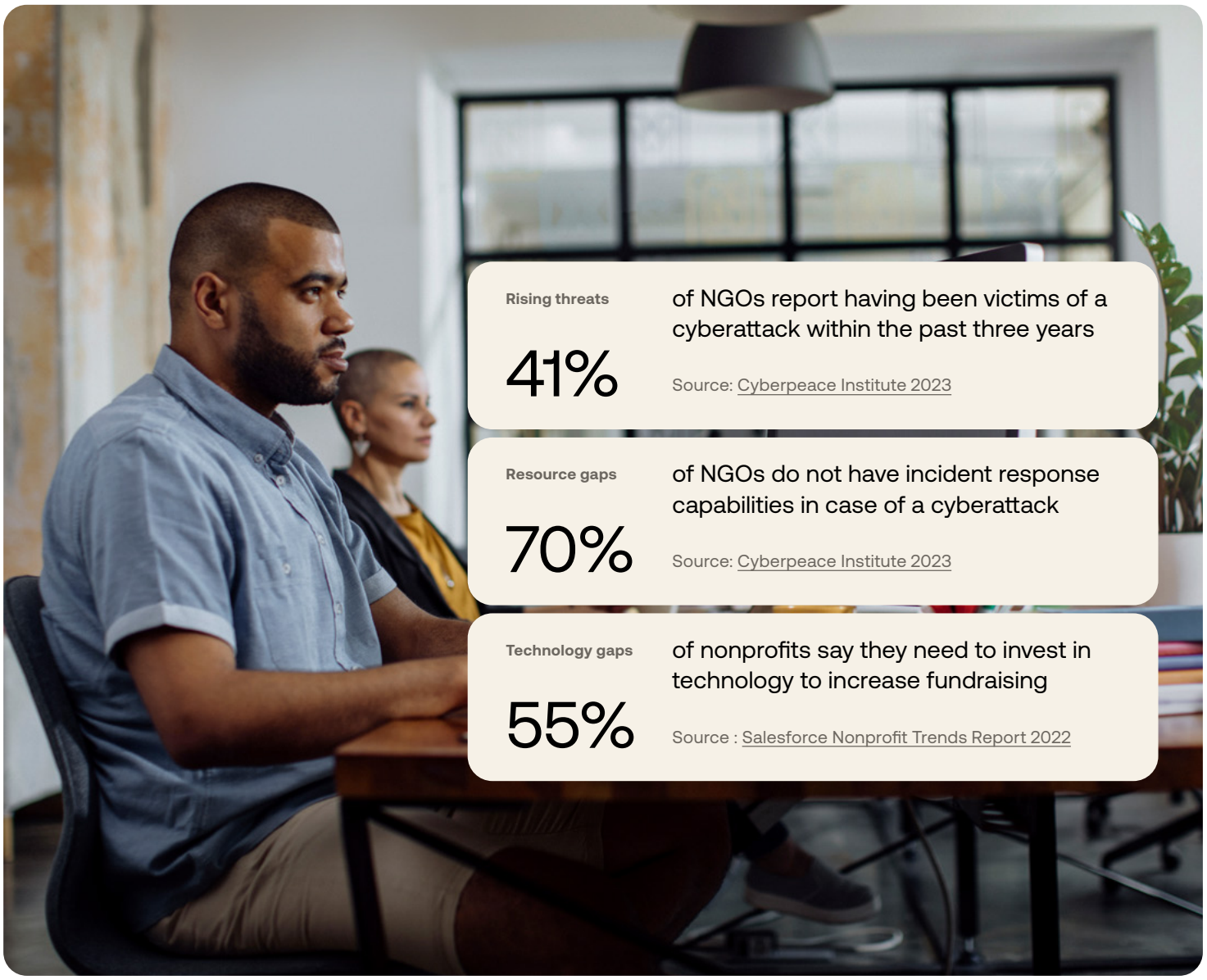
okta



Identity Maturity for Nonprofits

Practical Steps and Solutions for Every Stage

Effective Identity management enables nonprofits to secure sensitive data, streamline operations, and provide seamless experiences for staff, volunteers, and donors. This guide offers benchmarks and recommendations to help your organization improve its Identity management capabilities from wherever you stand today.

Why Identity and access management is needed

Your end users need frictionless access to the tools that allow them to deliver services and access critical resources. At the same time, you need to ensure that your communities' sensitive data is protected. Identity plays a crucial role in helping nonprofits achieve their goals and missions.

Stronger cybersecurity

Identity is the No. 1 attack vector in today's threat landscape and nonprofits hold sensitive data, like that of vulnerable populations.

31%

of nonprofits have measures to handle sensitive personal information

Salesforce Nonprofit Trends Report 2023

Increased revenue

Nonprofits compete for donors' attention and Identity creates a smoother experience that leads to higher engagement.

60%

of users are inclined to spend more when login is simple, secure, and frictionless

Okta Customer Identity Trends Report 2023

Lower costs and increased efficiencies

Identity platforms offer consolidation, integration, and automation that help improve IT and employee efficiency and optimize software investments.

22%

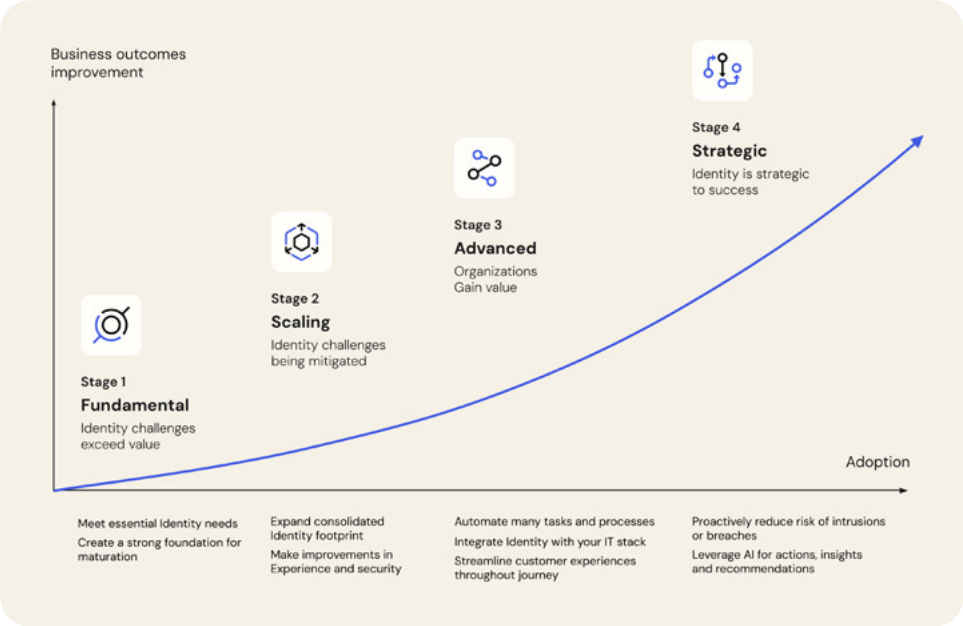
Organizations that invest heavily in automation can reduce costs by 22%, compared to laggards

Bain and Company 2023

The Nonprofit Identity Maturity Model

This model is based on patterns and collective best practices observed across thousands of Okta customers. As nonprofits increase Identity adoption, they also increase operational efficiencies, cost savings, and protection against threats.

While the stages are presented linearly, your Identity maturity journey may look different, and you may not fit entirely into one stage. Adopting or advancing any component of Identity is valuable, and this guide is meant to help you prioritize where to start improving.



Stage 1 - Fundamental

At the earliest stage of their Identity journey, nonprofits may struggle with inefficiencies and security threats due to disconnected Identity solutions. The focus at this stage is on meeting essential Identity needs (e.g., onboarding users into a single portal, implementing some Identity security controls, etc.) while creating a strong, reliable foundation.

Identity challenges

- Lack of visibility into application access controls
- Considerable login friction
- Security risks due to password sprawl, siloed user stores, and no centralized policies

Recommended actions


Consolidate user data into a central directory


Document Identity-related processes


Implement basic password policies and self-service resets


Conduct security awareness training for staff and volunteers

Recommended products and features

- Universal Directory
- Basic Single Sign-On (SSO) and Multi-Factor Authentication (MFA)
- Basic security encryption and hashing
- Basic access policies for APIs

Stage 2 - Scaling

In Stage 2, nonprofits may deliver more digital services, maintain online portals, and consolidate Identity solutions. Now, the focus is on expanding a more consolidated Identity footprint to new apps, services, use cases, and internal and external users.

Identity challenges

- Manual onboarding and offboarding impacts productivity and user experiences
- Performance or availability issues due to spikes in demand, on-premise authentication elements, etc.
- Security gaps due to limited MFA, over-permissive access policies, or a focus on donor/member experience over security
- Multiple apps/portals with inconsistent login experiences

Recommended actions


Automate basic user lifecycle management (e.g., onboarding/offboarding)


Harden Identity infrastructure to handle spikes and demand increases


Develop an Identity strategy aligned with organizational goals


Implement strong MFA and coarse-grained access control

Recommended products and features

- SSO capabilities for your entire staff/volunteers and external users
- Lifecycle Management
- MFA with stronger factors (biometric or passwordless)
- Role-Based Access Control with dynamic access policies

Stage 3 - Advanced

Nonprofits in Stage 3 are moving from reactive to proactive in threat prevention. Identity automation helps improve threat response and security posture by removing the risks associated with human error. At the same time, integration with other systems enables further automation and a better view of external users. Improving experiences for volunteers, partners, donors, members, and communities is also a focus.

Identity challenges

- Inefficient operational processes, beyond on- and offboarding, that impact experience and can introduce errors
- Supporting a variety of use cases without burdening the organization
- Meeting high donor/member expectations for frictionless, trustworthy experiences
- Security risks associated with remote workers, more sophisticated cyber threats, and larger threat surface

Recommended actions

Enforce least-privilege access to APIs, critical infrastructure, and applications

Leverage out-of-the-box integrations with marketing, CRM, HR, privacy/compliance systems, etc.

Develop self-service portals for various user groups and verify external user identities during onboarding

Establish Identity governance and compliance processes

Extend passwordless authentication to user touchpoints (devices, apps, accounts) and ensure phishing resistance

Recommended products and features

- Adaptive MFA
- Identity Threat Detection and Response (ITDR)
- Identity Security Posture Management (ISPM) tools
- Identity Governance and Administration (IGA)
- Automated user account linking/merging

Stage 4 - Strategic

For nonprofits in Stage 4, Identity is an essential strategic advantage for achieving mission-aligned outcomes. They focus on optimizing Identity infrastructure to support operations and mission goals, integrating Identity with their security tools, and implementing continuous reviews to better detect and respond to threats in real time. They often use AI to drive a better user experience and proactively improve Identity security.

Identity challenges

- Achieving a fully integrated Identity ecosystem
- Adapting quickly to market changes, donor patterns, regulations, etc.
- Legacy standing privileges across applications
- Identity misconfigurations

Recommended actions

Unify Privileged Access Management (PAM), Identity Access Management (IAM), and IGA for better visibility, control, and faster threat response

Utilize AI/ML for anomaly detection, risk assessment, and easier development

Create personalized, AI-driven experiences based on user attributes and behavior

Recommended products and features

- PAM
- Fraudulent Identity remediation
- Security operations workflow automation
- User behavior analytics
- Fine-Grained Authorization

Practical steps for nonprofits

1. **Assess your current state of Identity & cybersecurity**
   - Evaluate your existing Identity practices against this model or Okta's more detailed Guide for your Identity Maturity Journey
   - Determine which stage(s) best describe your current situation
   - Use assessment tools, such as those from TechSoup or NTEN, and Okta's Identity Security checklist

2. **Set realistic goals that align with your mission and develop a roadmap**
   - Align Identity initiatives with broader organizational goals
   - Begin with core Identity features and gradually add more advanced capabilities as your needs grow
   - Prioritize quick wins that can demonstrate value

3. **Get board and leadership approval for new solutions**
   - Quantify the value of any new technology needed and make a business case
   - Follow the framework in Unlocking Nonprofit Board Understanding

4. **Integrate with existing technology**
   - Look for Identity solutions that integrate well with your current software (e.g., donor management, volunteer coordination)
   - Hire agencies for implementation support

5. **Leverage programs and resources for nonprofits**
   - Explore Identity solutions with nonprofit discounts or grants
   - Seek volunteer expertise from tech-savvy supporters and pro-bono consultants to help navigate more complex Identity projects
   - Utilize services from nonprofit technology consortiums like Tech Soup and its Digital Resilience Program, NetHope, and NTEN
   - Harness open-source tools if you have technical expertise

6. **Improve cybersecurity education for users**
   - Regularly train staff and volunteers on security best practices
   - Communicate the importance of Identity management to all stakeholders

7. **Monitor and adapt**
   - Regularly assess your progress and adjust your strategy as needed
   - Stay informed about emerging Identity trends and threats

Improving your nonprofit's Identity maturity is a journey that yields significant benefits in security, efficiency, and user satisfaction. Understanding your current state and taking incremental steps can create a solid foundation for growth and impact. Progress is more important than perfection — each improvement you make strengthens your organization's ability to fulfill its mission securely and effectively.

Okta can help

Okta's Workforce and Customer Identity Clouds safely connect internal and external users to applications across different devices and directories. Okta has helped countless nonprofits adopt its Identity solutions to secure and simplify their operations — with enthusiastic buy-in from executive leadership and boards. To learn more about support for nonprofits, please visit our nonprofit page.

Extending security beyond Identity

Nonprofits need multiple solutions to enforce fine-grained rules and policies that secure every user, device, and connection. Okta offers integrations with best-of-breed technologies to help you enable a Zero Trust architecture and achieve holistic security, whether or not you have a Zero Trust strategy in place.

Okta + AWS, Crowdstrike, and Zscaler

Combining Okta with Amazon Web Services (AWS), CrowdStrike, and Zscaler gives you a complete, integrated security ecosystem that includes IAM, cloud infrastructure, endpoint protection, and secure connectivity.

Identity

- User Identity verification
- MFA enforcement
- Device context

Application/data

- Private app/infrastructure access
- AWS S3 access

Device

- User device ZTA score

Network

- Inline policies
- Device trust levels
- SCIM provisioning with Okta