Whitepaper

A Guide for Your Identity Maturity Journey

A roadmap for raising productivity, user experiences, and security through Identity

Table of contents

Identity fuels business goals

Digital Identity was once a simple service that managed usernames and passwords. Now, Identity is an enabler of modern business. It's an engine that empowers organizations to securely engage with their workforce, clients, and partners, wherever they happen to be, on whatever device they are using, and track and control that engagement. Identity is woven into every aspect of our online-first world. It can play a part in delightful or disappointing user experiences, improve or obscure security investigations, save or cost IT time and money, and contribute to or complicate governance, risk and compliance (GRC) initiatives. As a result, Identity also has a role to play in many business outcomes, including operational efficiency and cost control, revenue growth, and strengthening cybersecurity. With so much riding on it, it's no surprise that many organizations struggle to modernize and improve their customer and workforce Identity services.

Identity can transform how businesses interact with users, thereby contributing to the following business goals:

Increased revenue:

Many industries are competing on the customer experience, and Identity is an integral part of optimizing that experience.

60%

of users are inclined to spend more when login is simple, secure, and frictionless.[1]

Lower costs and increased efficiencies:

The consolidation, integration, and automation that an Identity platform offers can help improve IT and employee efficiency, optimize software spend, and get offerings to market faster.

22%

Companies that invest heavily in automation are able to reduce costs by 22%, compared to laggards.[2]

Stronger cybersecurity:

As the No. 1 attack vector in today's threat landscape, Identity has a vital role in your security stack.

61%

of businesses now see managing and securing digital identities as a top three priority of their security program.[3]

[1] Okta Customer Identity Trends report, 2023

[2] Bain and Company, 2023

[3] 2023 Trends in Securing Digital Identities report, Identity Defined Security Alliance

The Identity Maturity Model

Research[4] shows organizations who are leaders in Workforce Identity maturity are

3.9x

as likely to say their Identity solutions enable business agility

3.4x

as likely to say their Identity solutions help significantly with incident respomse

3.6x

as likely to say their Identity solutions enable employee productivity

3.2x

as likely to say their Identity solutions help to significantly mitigate threats

Okta's Identity Maturity Model is a framework for assessing the current state of your Identity capabilities and effectiveness, creating a plan to improve them, and measuring ongoing success and value. By understanding the maturity of your Identity landscape and how advancing maturity will help you achieve business outcomes and realize more value, you'll know how to focus your efforts and investments best.

Based on patterns and collective best practices we've observed across thousands of Okta customers, we've developed a comprehensive maturity model that provides both a journey and evaluation criteria for all your Identity-related actions. This paper discusses the maturity aspects of Workforce Identity for employees, contractors, and partners, as well as Customer Identity for consumers, suppliers, and other constituents. Research and testimonials from our customers both show that the further organizations are in their Identity maturity, the more Identity contributes to business success.

Assessing Identity maturity and evaluating success

The first step on this journey is to conduct a thorough and realistic assessment of your company's existing approach to Identity. Our evaluation examines Identity through the lens of three categories: operational agility, end-user experience, and security and compliance. As you mature your Identity, consider how your efforts contribute to business outcomes. By consistently measuring key performance indicators (KPIs) and mapping them to business outcomes, such as the ones presented in Table 1, you'll be able to show progress and secure additional organizational buy-in.

Beyond these three categories, each stage suggests actions to define, refine, implement, and evaluate an organization-wide Identity strategy.

[4] The benefits of a mature approach to Identity Management, Enterprise Strategy Group, commissioned by Okta

Category	Description: Ability to	Metrics for Evaluating Identity Success	Contribution to business outcomes
Operational Agility	**Develop, deploy, and manage Identity-related services and flows,** e.g. • Integrate Identity into new digital properties or applications • Manage workforce lifecycle • Deploy new Identity features or enhancements • Quickly roll out new offerings to customers • Scale easily and quickly to meet fluctuations in demand	• IT FTE hours dedicated to Identity administration and support • Time to adopt and deploy applications • Cost or time spent maintaining Identity infrastructure • Number of help desk tickets related to access issues or requests for applications • Time to resolve Identity help desk issues • Time to market for customer applications	Cut costs and increase efficiency • Build and maintain Identity with less effort • Simplify M&A for faster time to value Increase revenue • Get to market faster
End-user Experience	**Deliver effective, desirable, and convenient user experiences,** e.g. For everyone: • Consistent, reliable experiences across digital properties and channels For workers: • Seamless remote access • Applications available on day one • Efficient self-service for requesters and reviewers For customers: • Low-friction experiences for registration, sign in, etc. • Self-service • Personalization	• Employee satisfaction (eSAT) scores • Customer experience metrics (e.g. NPS, CSAT) • Time spent by users logging in or responding to step-up authentication prompts • Time spent by employees waiting for access to new applications, or being onboarded • Customer abandonment rates at registration and login • Customer conversion rates (visitor to registered account) • Minutes of unplanned downtime per month	Increase efficiency • Streamline end user access Increase revenue • Increase sign up and login conversions • Personalize customer experiences • Create seamless omnichannel experiences • Simplify onboarding of enterprise customers
Security & Compliance	**Proactively mitigate and remediate threats, maintain least privilege, and support regulatory compliance,** e.g. • Secure workforce and customer access • Reduce Identity threat surface • Support Identity governance initiatives • Manage privileged access • Support Zero Trust practices • Support privacy requirements • Protect against Identity fraud	• Number of Identity-related security incidents • Time and costs to detect and respond to Identity-related security incidents and breaches • Time and costs to deliver audit- and compliance-related reporting • Employee adoption of advanced authentication • Number of account takeover (ATO) incidents	Cut costs and increase efficiency • Simplify governance and compliance • Optimize software spend • Increase revenue • Increase customer trust without impacting the experience Strengthen cybersecurity • Proactively mitigate Identity threats • Stop phishing attacks • Enable consumer trust

Charting your journey stage-by-stage

Okta's Identity Maturity Model has four progressive stages that itemize various Identity capabilities and how you can use them to help achieve business outcomes and organizational value. At each stage we outline typical challenges organizations face, provide guidance on next steps to take to address the challenges and progress to the next maturity level, and the expected benefits. For each stage we suggest actions to build, implement, and evaluate an organization-wide Identity strategy. While there is no one-size-fits-all approach to Identity, this approach is flexible enough to provide guidance for any business interested in advancing its Identity posture.

Identity Maturity Model

Stage 1 - Fundamental

Consider Identity holistically, rather than a collection of functions

At the earliest stage of Identity maturity, organizations may be

- Beginning the process of extending digital services or online portals to their customers
- Dealing with inefficiencies and a large threat surface due to disconnected Identity solutions for their workforce and partners

With no defined Identity strategy, developers spend considerable time and resources on building and maintaining on-premises or homegrown Identity services. Workforce Identity is fragmented into multiple stores and systems resulting from mergers and acquisitions (M&A), cloud expansion, and legacy applications. User experience is poor: customer sign-ups are basic and inconsistent across properties; for workers, limited federation and reliance on multiple passwords impacts productivity. Identity reliability and availability is a concern; automation is minimal or non-existent. Any integrations with other systems are limited or cumbersome and demand considerable manual effort from administrators. Identity sprawl and the resulting lack of visibility increases security risks, and any Identity security is reactive.

At this stage, the focus is on meeting essential Identity needs (e.g., onboarding customers into a single portal, implementing some Identity security controls) while creating a strong, reliable foundation for maturation.

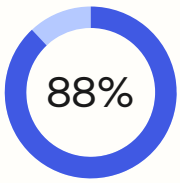
Strategy steps to take at this stage:

- Create an inventory of on-premises and cloud apps in use in the organization
- Consider aligning customer and workforce Identity programs around shared business and governance goals

Building and maintaining in-house Customer Identity impacts time to market[5]

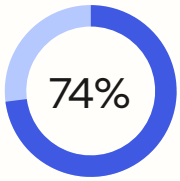
3rd most time-consuming

Authentication is the third-most time-consuming application to build in-house and maintain



of organizations that use a third-party SaaS platform for authentication reported reducing their time to market

vs.



of organizations that built authentication in-house

[5] How Development Teams Purchase SaaS, SD Times, commissioned by Okta

Category	Identity Challenges	Actions to Take	Business Benefits
Operational Agility	• Building/maintaining on-premises/ homegrown/fragmented Identity services is difficult and time-consuming for admins and developers	• Implement a unified user directory to consolidate and synchronize user repositories across legacy directories and systems of record • Implement basic Identity administration UI for user lifecycle	Reduce IT time spent • Maintaining and synchronizing user stores • Managing user/group access
End-user Experience	• Reliability/availability issues • Considerable login friction; no customizable user experiences • Disparate Identity solutions per business unit	• Adopt a high availability (HA) infrastructure with failover, disaster recovery, and SLA standards greater than 99.9% • Deploy basic workforce single sign-on SSO and authentication to cloud apps • Deploy basic customer SSO with a few social authentication options to leverage existing credentials • Implement simple self-service functions (e.g., password recovery)	• Improve workforce productivity and/ or customer utilization due to faster application adoption and access • Reduce customer friction with self-service options for basic account management
Security & Compliance	• Security risks due to password sprawl, lack of visibility into application access controls, siloed user stores, no policy enforcement, etc.	• Install an authorization server compliant with modern standards and basic access policies for APIs • Secure Identity data with basic security encryption and hashing • Establish workforce multi-factor authentication (MFA) that includes RADIUS, LDAP to support modern and legacy apps • Establish some workforce access policies that reflect user group needs and network zones	• Strengthen workforce security posture • Reduce customer account lockouts resulting from malicious attacks

Stage 2 - Scaling

Expand Identity footprint and capabilities, begin automation

At this stage, organizations may have

- Launched more than one customer application or portal, and are committed to delivering more
- Realized some success with workforce Identity consolidation and are looking to expand to more apps and implement additional Identity capabilities

Now, the focus is on building on the success of stage one and expanding the consolidated Identity footprint to new apps, services, use cases, and users. As organizations deliver new digital services to compete for market share and grow their customer base, their focus shifts to creating differentiated, trustworthy experiences for both consumers and business customers.

For organizations with critical on-prem IT infrastructure and proprietary technology, expanding Identity functions to these resources will improve user experiences, administrative processes, and security posture.

As the footprint grows, organizations must ensure their Identity infrastructure can handle increases in demand without compromising service quality or requiring IT to constantly manage scaling and support. Companies should also start automating some Identity processes, so that expansion doesn't place a huge burden on IT and application owners. With a majority of businesses adopting a Zero Trust approach to cybersecurity, this is a good time to start leveraging Identity to foster that initiative.

Strategy steps to take at this stage:

- Establish Identity alignment and communication between IT, technology, and security teams to define areas of ownership and expertise
- Evaluate Identity gaps to drive remediation and investment plans

Category	Identity Challenges	Actions to Take	Business Benefits
Operational Agility	• Manual onboarding and offboarding for workforce, customers, and partners • Fragmented Identity repositories from legacy systems are difficult to maintain • Spikes/increases in demand lead to performance or availability issues	• Begin to automate user lifecycle management and provisioning for onboarding and offboarding, and for managing downstream app access permissions, etc. • Minimize or consider retiring some legacy systems that: are difficult to maintain/upgrade; have distinct user stores; have no or difficult integration capabilities; have no SSO/federation capabilities • Integrate Identity with applications using standards such as SAML OIDC, OAuth2, etc. • Begin to adopt some SDKs and APIs • Ensure infrastructure can reliably handle spikes/increases in demand without compromising service quality	Reduce • Time and cost to maintain identity infrastructure • Help desk tickets relating to access issues • Maintaining and synchronizing user stores • Managing user/group access • Time developers spend scaling Identity Faster provisioning and deprovisioning of users Simplify M&A for your workforce and customers
End-user Experience	• Multiple apps/portals with inconsistent login experiences • Onboarding delays for new employees • Availability of secure authentication due to on-premise RADIUS servers, etc.	• Extend customer login integrations to other social Identity providers, such as Apple, Google, etc. • Support SSO federation for customers, partners, and contractors that have existing identities in third-party Identity providers • Minimize customer sign-in and registration friction by only prompting for required attributes • Extend workforce SSO to on-prem business-critical applications • Implement workforce passwordless authentication • Launch more self-service functions	• Reduce user friction with better sign-in and registration experiences • Improve workforce productivity and satisfaction with birthright access to key applications and faster access to other apps • Improve reliability with fewer outages due to on-premises or non-redundant servers
Security & Compliance	• Global access policies result in a too-permissive workforce access environment • Limited workforce MFA creates security gaps • Customer experience goals get in the way of security	• Consolidate workforce access controls across cloud and on-prem apps • Implement role-based access control (RBAC) • Extend strong workforce MFA (with possession or biomentrica factors) to partners and contractors and across on-prem business-critical apps, or implement passwordless access • Implement customer MFA with possession or biometric factors, or implement passwordless access • Take initial steps towards Zero Trust (e.g. dynamic access policies) • Integrate with standards-based API gateways for consistent view of consumer authorization • Introduce some audit and monitoring tools	• Strengthen security posture • Increase compliance with least-privilege access mandates and MFA access controls (e.g., SOX) • Reduce the time and cost to prepare for audits and compliance reviews

Stage 3 - Advanced

Increase automation and integration, elevate experience

Organizations at this stage are gaining significant value from Identity. Their focus is on

- Streamlining the customer experience to optimize conversions
- Beginning to integrate Identity with their broader technology stack to improve efficiency
- Becoming proactive with Identity security

Integrating Identity with other systems allows you to automate tasks and processes and gain greater visibility of users and their environment. For example, deep integrations with HR systems enables organizations to automate creating user identities, onboarding, offboarding, and workforce provisioning – improving worker productivity, increasing IT admin efficiency, and reducing software costs and security risks due to overprovisioning. Integrating customer Identity with marketing and data engines consolidates data silos and offers a single view into user profiles, enabling a consistent brand experience across channels. Organizations can also learn more about customers and their preferences, enabling personalization. Increasing automation also enables their developers and IT teams to focus on priorities that move the business forward.

As organizations grow their operations and digital footprint, they are increasingly targeted by more sophisticated cyberattacks, and a variety of security tools have cropped up in response. Identity threat detection and response (ITDR) and Identity security posture management (ISPM) tools help close security gaps and improve response to threats. By integrating these capabilities with your Identity system, you can assess and automatically respond to changes in Identity risk.

Strategy steps to take at this stage:

Collaborate with diverse teams on workforce and customer Identity strategy

Adopt formal, ongoing processes for evaluating Identity security posture

Measure and make decisions based upon Identity-related KPIs

Category	Identity Challenges	Actions to Take	Business Benefits
Operational Agility	• Inefficient business processes that lag technology advancements, with manual activities that introduce delays and risk of errors • Supporting a variety of Identity use cases without burdening developers	• Automate most lifecycle management processes including birthright provisioning and access requests to minimize the need for developer and IT intervention • Leverage some out-of-the-box integrations with business and marketing systems • Automate worker access recertification based on role or job changes • Support a variety of SDKs and APIs with advanced support and documentation	Reduce time • IT and engineering spend on custom integrations • IT and GRC teams spend running manual recertification campaigns and audits • Managers and app owners spend reviewing access Adopt new business systems and applications faster
End-user Experience	• High customer expectations for frictionless, consistent, seamless experiences • Workforce access friction due to: rigid access policies that don't adapt to users or context; time-consuming processes to access apps	• Ensure resilience with redundant servers and load balancers • Automate user account linking/merging • Use progressive profiling to capture customer attributes over time and enrich profiles • Implement passwordless for all user touchpoints (devices, apps, accounts) and using Passkeys, hardware or software authenticators where appropriate • Improve customer onboarding with Identity proofing and account verification • Enable workforce self-service access requests	• Create seamless omni-channel customer experiences • Increase sign-up and login conversions with better targeting and personalization • Increase employee productivity due to more self-service automations and faster access • Reduce fraud with advanced account verification
Security & Compliance	• Risks associated with remote workers, their devices and networks • Targeted by more and sophisticated cyber threats	• Extend workforce high assurance MFA to computer login • Ensure phishing-resistant MFA for workforce across all resources • Institute attribute-based access control (ABAC) • Integrate with ITDR and ISPM tools • Implement secure passwordless access to critical infrastructure such as servers, Kubernetes clusters, databases, etc. • Deploy Identity security posture management to discover risks due to misconfigurations, over-permissioned users, etc. • Adopt continuous authentication to support Zero Trust and make access decisions with the latest data • Implement automated security responses to identity risks • Adopt recurring (scheduled) user access recertification to enforce least-privilege access • Integrate with privacy and compliance tools to track customer preferences	• Reduce threat surface • Simplify governance and compliance by automating access reviews and access request flows • Stop phishing attacks

Stage 4 - Strategic

Use Identity to gain a strategic advantage

At this stage, organizations view Identity as strategic to success and an important contributor to business outcomes. They often have a robust, global digital presence with teams working collaboratively to continually refine Identity initiatives that empower their workforce and build better relationships with their customers across multiple channels.

At this stage, organizations are focusing on

- Optimizing Identity infrastructure to support efficiency and operational margins
- Integrating Identity with their security stack to detect and respond to threats in real time
- Taking advantage of artificial intelligence (AI) and their cloud footprint to drive a superior user experience and proactively improve Identity security

When Identity is fully integrated into the technology stack, organizations can collect, normalize, and correlate data across their infrastructure. Identity becomes the primary control plane for administering access to resources and a key element of any cybersecurity strategy. From a GRC perspective, Identity integration provides visibility and fine-grained access control over which users and devices have access to specific digital resources and permissions in their organization, as well as the ability to better track customer preferences with respect to privacy. Combined with widespread Identity automation and AI for insights and recommendations, organizations can more easily and quickly adapt to changing customer expectations, business and regulatory requirements, and the threat landscape.

Strategy actions to take at this stage

Have mature governance and operational practices in place that ensure Identity continually evolves to meet business needs and deliver value

Category	Identity Challenges	Actions to Take	Business Benefits
Operational Agility	• Gaining unified view of Identity across cloud, on-premise, and hybrid cloud environments • Adapting to changing market needs, user patterns, regulations, etc.	• Centralize all Identity data across users, applications, and entitlements • Fully automate policy, user lifecycle management, and Identity-related operations and threat response workflows • Leverage AI to recommend stronger Identity security and governance, better user experiences, and easier configuration and development	• Get to market faster with Improved IT, admin, and developer efficiency
End-user Experience	• Different customer experiences across devices/channels • Understanding customer behaviors for targeting and security	• Ensure customizable and extensible customer access experiences across channels • Trigger contextualized questions during customer registration and login to capture zero-party data	• Create seamless/ omnichannel experiences • Hyper personalize with integrated zero-party data
Security & Compliance	• Legacy standing privileges across applications and infrastructure • Cloud or other identity misconfigurations • Responding quickly to security events	• Ensure zero standing privileges remain; manage shared credentials for privileged resources in secure vaults • Unify Identity security (IAM, PAM, and IGA) • Ingest signals from third-party security tools for better threat insights • Deploy risk-based, fine-grained authorization • Automate user access recertification based on risk signals • Ensure infrastructure can dynamically scale with demand spikes and demonstrate compliance with regulations related to reliability and security	• Proactively mitigate and remediate Identity threats • Reduce time to detect and respond to threats • Increase trust without sacrificing the customer experience • Enable consumer trust through advanced security and fraud protection

Unlocking Identity's business value

Once you know where your organization is on the Identity maturity journey, you can better assess next steps and monitor success. By understanding how Identity helps support innovative digital experiences, protects against security threats, and drives business growth, you'll be a step ahead of your competition.

As the leading independent Identity partner, Okta has worked with organizations around the world across a variety of industries to further their digital transformation and secure access, authentication, and automation goals. Okta frees up your organizations' time and resources so it can focus on core products and services while we monitor the Identity and security landscape and deliver innovations.

For a glossary of Identity terms, please visit https://www.okta.com/resources/identity-and-access-management-glossary/