

# A Comprehensive Guide for Your Customer Identity Maturity Journey

---

Okta Inc.

---

100 First Street

---

San Francisco, CA 94105

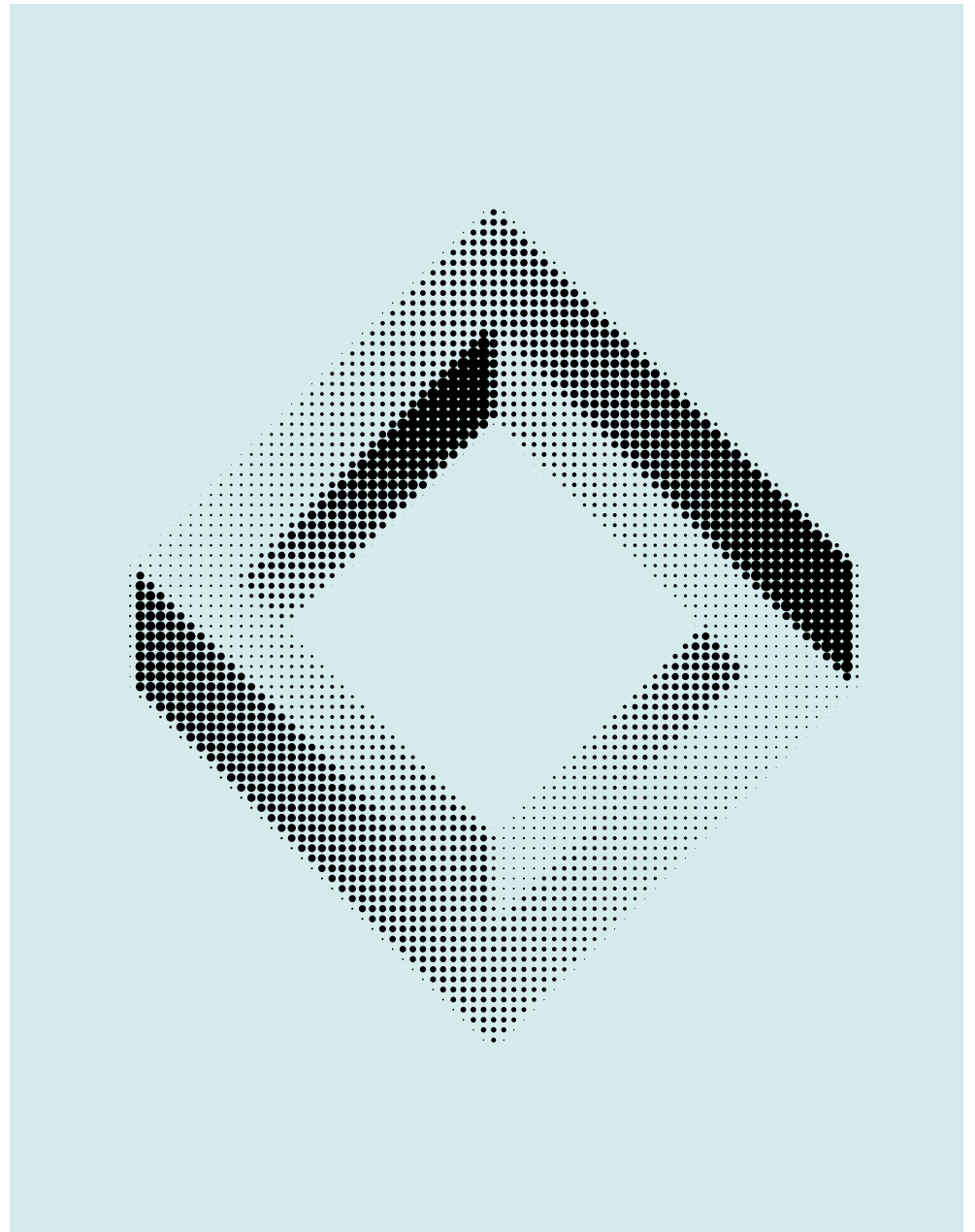
---

[info@okta.com](mailto:info@okta.com)

---

1-888-722-7871

---



# State of modern identity

Several recent converging trends have made identity and access management (IAM) both a necessity and a ubiquitous enabler for any modern business. More and more companies are moving towards distributed, dynamic workforce models to reach and retain top talent, while increasingly delivering their products and services digitally in search of market growth. To stay competitive and deliver the secure, seamless user experiences demanded by today's online-first world, businesses of all sizes are exploring the value of modern identity technologies in addressing these workforce and customer-facing challenges.

Each organization's progress in tackling these demands varies based on its holistic approach to identity. And while the need for a robust solution is evident, the path towards an effective, successful implementation is often not. Some companies may have a mature workforce identity strategy in place, but are just starting to launch new digital experiences and safeguard customer identities. Others struggle to move away from legacy or disjointed user authentication and other homegrown services — hindering their ability to innovate and creating undue budgetary pressures across the organization.

## A cohesive, future-proof path forward

It can be challenging to know where to start when trying to weave a future-proof identity fabric throughout your business. Many teams lack the expertise, strategy, and tools to effectively address their litany of requirements, including walking the tightrope between user experience and security.

Based on patterns and collective best practices we've observed across thousands of Okta customers, we've developed a comprehensive maturity model that provides an optimal journey and evaluation criteria for all your identity needs. This series of papers starts with customer identity, which centers on external users (such as consumers, suppliers, and other constituents), while traditional IAM manages identity and access for workforce users (such as employees and partners).

Read on for guidance about specific steps to take at each stage throughout the customer identity maturity journey, so you can get on the path towards delivering superior & new digital experiences, protecting against security threats, and improving operational efficiencies by modernizing IT & infrastructure. Our approach is flexible enough to address varying business needs, with the aim of helping any company advance its identity posture.

# What is an identity maturity model?

Okta's Identity Maturity Model (IMM) 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 IAM landscape and through evaluating the identity & security capabilities required to achieve your organization's long term business objectives (i.e. where you're at and where you're going), you'll know how to best focus your efforts and investments. This will ultimately position your business to more easily scale in response to new identity and security requirements, as well as shifting end-user demands.

## Assessing key areas of identity maturity

The first step on this journey is to conduct a thorough and realistic assessment of your company's existing approach to identity, including key capabilities and challenges. This evaluation should examine five critical categories: agility, experience, security, reliability, and strategy.



### Agility

Ability to develop, deploy, and maintain identity-related services and flows



### Experience

Ability to deliver effective, desirable, and convenient experiences to end-users



### Security

Ability to proactively and effectively mitigate and remediate security risk and incidents



### Reliability

Ability to provide a resilient, high performing, future-ready identity service at any scale



### Strategy

Ability to plan and deliver holistically, intelligently, and with a focus on innovation

Specifically, as it relates to customer identity maturity, these key assessment areas take the following form:

**1. Agility** in developing, deploying, and managing identity-related processes and services:

- Are you able to quickly and cost-effectively deploy new identity features and enhancements?
- Can your developers easily integrate applications to your identity service?
- Does your identity service provide extensive SDKs and APIs to ensure fast onboarding and efficiencies for new developers?
- Do administrators have an intuitive and centralized service for managing external identities and their access requirements?

**2. Delivery of convenient, desirable, and tailored digital customer experiences:**

- Do external users have simple, low-friction experiences for all required identity services such as registration, sign in, password reset, etc.?
- Do you provide a consistent and unified access experience for them across digital properties and channels?
- Can customers self-serve to resolve authentication-related issues?
- Are you able to capture and integrate user data incrementally along the customer journey?

**3. Mitigation and remediation of security risks and incidents:**

- Are your external users' identity credentials adequately protected?
- Are you leveraging modern, sophisticated identity tools to secure customer access experiences?
- Do you securely store your customers' personally identifiable information (PII) and preserve privacy in accordance with regulatory requirements?
- Can your internal teams quickly uncover and resolve identity-related security incidents?

4. Ability to provide a **reliable**, high performing, future-ready identity service at any scale:

- Do you experience outages that impact your revenue-generating business and / or customer experiences?
- Is your identity service able to handle large spikes in user traffic without interruptions, even when unexpected?
- Are you able to scale your service to address demand fluctuation in a timely and cost-effective manner?

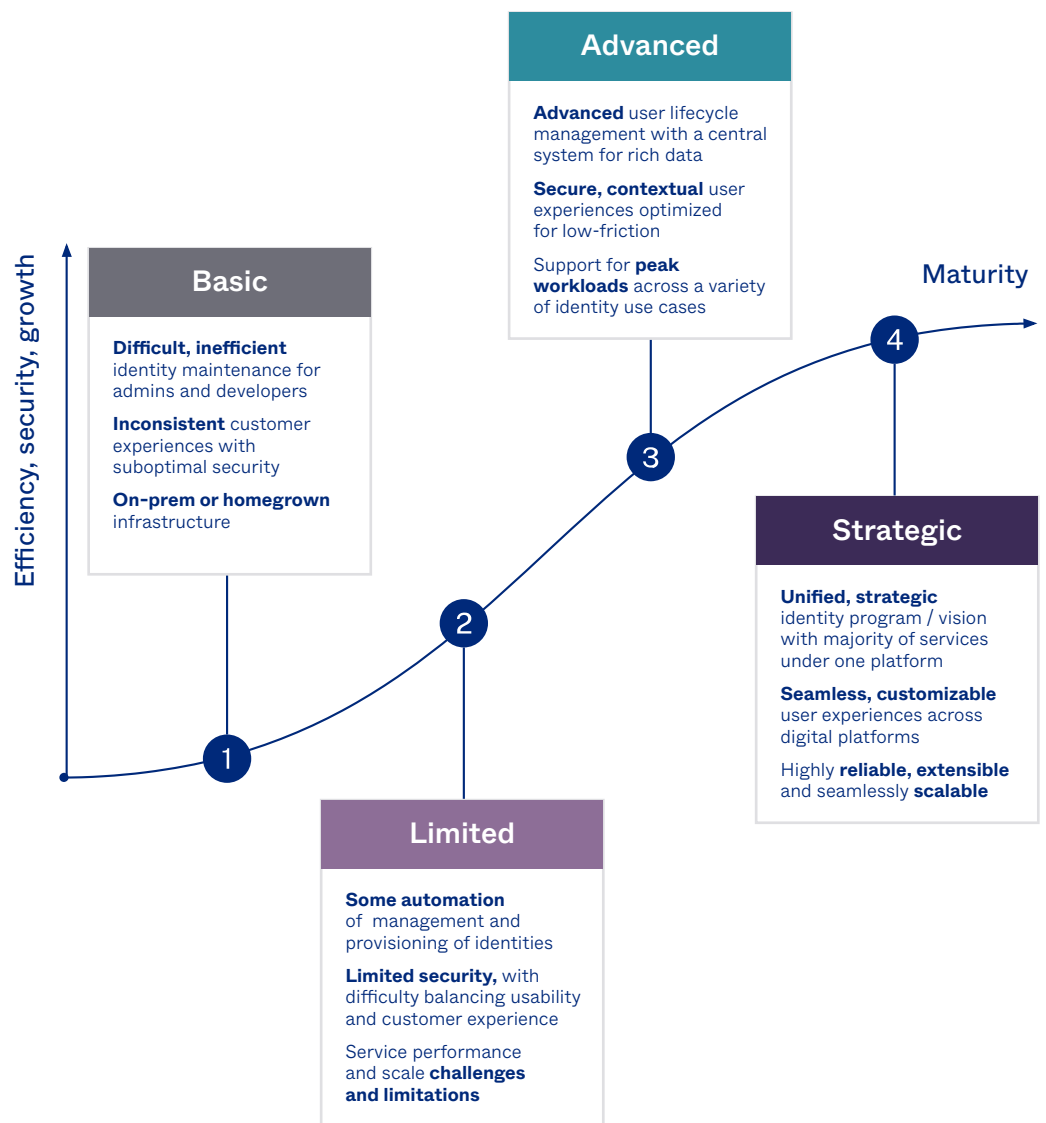
5. A unified, strategy, focus, and vision for customer identity innovations across the business:

- Is your identity strategy aligned across all of your key business units?
- Is it fully-funded, multi-year, and supported by executive buy-in?
- Do you have a dedicated team to manage and administer your identity service?
- Can you proactively measure and maximize the ROI of your identity services?

# Mapping the way to customer identity maturity

Now that we've discussed why and how you should evaluate the maturity of your customer identity capabilities, let's explore the four primary stages of Okta's IMM: basic, limited, advanced, and strategic. Each of these key steps towards customer identity maturity unlocks more value for your organization.

## The customer identity maturity journey



Our model provides guidance for launching a sustainable identity strategy and a starting point to evolve your organization from manual, inefficient, and fragmented identity functions to automated, intelligent, and scalable ones. Each individual business should determine what level of maturity it needs, and not all organizations will elect to reach Stage 4.

## Key metrics for evaluating customer identity success

As you journey through these four stages, it's important to know what good looks like. Be sure to consistently measure key performance indicators (KPIs) so that you can show progress over time across business outcomes such as:

### Agility KPIs

FTE time spent on identity administration, developing identity-related code, integrating identity into new digital properties, and customer support related to access issues; time to market

### Experience KPIs

End-user abandonment rates at both login and registration, conversions (visitor-to-registered account), and customer experience scores (e.g. NPS, CSAT)

### Security KPIs

Time to detect (and respond to) identity-related security issues, number and cost of account takeover incidents (ATOs), and the cost of a security breach

### Reliability KPIs

Minutes of unplanned downtime per month and the cost of 60 minutes of downtime on your business in lost revenue / customers; service level agreement (SLA) time

### Strategy KPIs

Annual investment in identity-related technologies, term of fully-funded identity program, identity service ROI and TCO

To see an example of how you can calculate ROI for your customer identity solution, visit <https://www.okta.com/roi/>

# Charting your journey stage-by-stage

In this section, we'll provide a more detailed overview of each maturity stage along with common goals and challenges. At the end of each section, we'll recommend steps to get started with increasing your identity capabilities en route to the next maturity level.

## Stage 1: Basic

### Goals & challenges

This is the earliest stage of maturity, with organizations typically just beginning the process of extending digital services, online portals, or software to their customers. These companies have the bare essential capabilities and architecture for managing customer identities and securing their data. Teams spend significant time and resources on building and maintaining a nascent on-premises or homegrown service, and lack expertise and insight around how identity fits into their broader business strategy.

At this stage, most companies are primarily concerned with onboarding customers to the system and digitally managing their identities. They've implemented only basic capabilities around authentication (user sign-in), authorization (access rules, policies), and user management (user sign-up).

### Our recommended steps and capabilities

If your organization is at this stage, we recommend implementing the following customer identity solutions and capabilities in order to proceed to the next level of maturity:



### Agility

- Basic identity administration user interface (UI) for user lifecycle and policy management (although you may still be highly reliant on manual execution from IT / development teams)





## Experience

- Basic end-user authentication with a single factor, such as password, PIN, etc.
- Basic single-sign-on (SSO) in the form of social authentication so end-users can leverage existing credentials from Google or Facebook
- Simple self-service functions, such as credential reset, password recovery, attribute management, and / or self-registration (although frequent Customer Support assistance may still be required)



## Security

- A simple user repository for storing identity data and attributes with basic security encryption and hashing
- Authorization server compliant with modern standards, e.g. OpenID Connect (OIDC) and Open Authorization (OAuth) 2.0, and basic access policies for APIs



## Reliability

- Basic identity infrastructure with limited high-availability architecture, failover and disaster recovery capabilities, service level agreement (SLA) standards, etc.



## Strategy

- Limited BU-specific strategies with disparate solutions
- An evaluation of whether identity is critical enough to build / maintain in-house or offload to third-party vendor

## Stage 2: Limited

### Goals & challenges

Once companies graduate from Stage 1, they have typically launched more than one application or portal and are committed to building and delivering great digital products and services repeatedly at scale. This requires a focus on creating differentiated and trustworthy customer experiences to effectively compete for market share and grow the user base.

Concurrently, companies must also bolster internal operational efficiencies to support business growth. For example, you might be looking to increase automation so you can boost productivity for admins and developers alike. This effort can stand to benefit from identity features such as intuitive admin portals and centralized, low-touch user lifecycle management.

At this juncture, businesses often begin to understand the myriad benefits of a fully automated and intelligent customer identity service — and at the same time, start realizing the deficiencies in their current systems that are preventing them from getting there.

### Our recommended steps and capabilities

In order to proceed to the next level of maturity, we recommend organizations implement the following customer identity solutions and capabilities:



#### Agility

- Partially automated user lifecycle management for onboarding and offboarding customers and partners, managing downstream system and application access permissions, etc.
- Some / limited support for modern protocols and open standards such as Security Assertion Markup Language (SAML), OIDC, OAuth, Fast ID Online (FIDO), etc.
- Some SDKs and APIs with limited support, guides, and documentation



## Experience

- Limited SSO federation capabilities and protocols to support third-party identity provider (IdP) usage for customers and partners with existing identities (e.g., AD, LDAP, SAML)
- Extended integrations with social identity providers, such as Apple, etc.
- Limited, partially customizable customer sign-in and registration experiences that only prompt for required attributes to minimize friction



## Security

- Multi-factor authentication (MFA) with limited assurance factors (e.g., SMS, email) and user context considered during authentication
- Audit and monitoring tools, such as coarse-grained reporting logs, for enhanced security and administration
- Integration with standards-based API gateway(s) for consistent view of end-user authorization



## Reliability

- Expanded identity infrastructure to support performance and reliability at scale
- A plan for bursts / spikes that often require ad-hoc investments and manual intervention



## Strategy

- Alignment and communication between diverse stakeholder teams leveraging customer identity technologies to define specific areas of ownership and responsibilities
- Realistic evaluation of customer identity gaps and requirements to drive development of remediation and investment plans

## Stage 3: Advanced

### Goals & challenges

An organization at this stage is typically fully focused on optimizing and scaling digital offerings, while safeguarding the security and privacy of end-users and their data. Customer expectations are high, with a growing mix of users demanding frictionless and personalized experiences. To deliver, organizations should invest in a plethora of advanced customer identity capabilities.

First, they must implement solutions that streamline the customer experience, so that users enjoy convenient, yet secure, access throughout the digital journey. This requires a variety of authentication options and intelligent access policies that minimize friction.

Also paramount is the ability to integrate identity within your broader technology stack (e.g., marketing engine, content management system, data management platform, etc.). When you're able to do this successfully, you can consolidate data silos and gain a single view into a customer's profile and data. This enables a unified and consistent brand experience, as well as rich data and analytics to learn more about customers and their preferences.

Lastly, organizations need to consider enhancing their backend identity systems and infrastructure by introducing more advanced automation and process efficiencies. This will minimize any intervention required from IT and developers, freeing up these teams for more important priorities that can help move the business forward.

### Our recommended steps and capabilities

At this stage, we recommend organizations implement the following customer identity solutions and capabilities in order to proceed to the next level of maturity:



#### Agility

- Advanced automations to codify a majority of user lifecycle management business rules and minimize the need for manual developer and IT intervention
- Some out-of-the-box integrations with business and marketing platforms / systems to track and identify customers across devices and channels
- A variety of SDKs and APIs with advanced support and documentation



## Experience

- Automated end-user account linking / merging to enable a single access experience for consumers with one login
- Advanced customizations and logic for customer authentication experiences
- Progressive profiling of customers to build tailored registration experiences that capture user attributes over time, lessening friction
- Passwordless technology using email magic links or WebAuthn to bolster user experience and eliminate credential-related identity attacks
- Sophisticated user onboarding with fully-integrated, best-of-breed identity proofing and account verification



## Security

- Intelligent MFA with adaptive features that leverage a variety of high assurance factors and behavioral inputs to assign risk and step up authentication only when needed
- Identity platform event and activity data for proactive risk detection and attack prevention
- Some out-of-the-box integrations with third-party tools / systems to capture and manage security events and signals
- Some out-of-the-box integrations with privacy and compliance tools to track customer preference and requirement



## Reliability

- Built-in service resiliency with redundant servers, load balancers, and high-availability infrastructure
- Built-in service buffers to handle traffic spikes of users, devices, etc. that need to be stored in a database



## Strategy

- Formal and ongoing processes, plans, and organizational ownership for evaluating identity posture
- Ability to track and quantify a variety of identity-related KPIs / metrics to demonstrate measurable improvement
- Trained, dedicated customer identity experts in-house

## Stage 4: Strategic

### Goals & challenges

Only a small percentage of companies advance far enough in their customer identity journey to reach Stage 4. Those that operate at this level have mature digital and omni-channel initiatives that optimize for both user experience and security, and they view identity as strategic to success.

Companies typically have a robust and growing customer base that is diverse and often global. These customers interact with your business via multiple channels, while demanding more advanced features, integrations, and identity capabilities for delightful yet trusted experiences. Different teams across the company work together to devise, develop, sell, and scale these digital offerings, but each has its own set of distinct requirements and priorities.

Addressing the varied and ever-evolving demands of both internal and external stakeholders at this stage is a balancing act like no other. As companies scale and evolve, so do customer expectations, the security threat landscape, regulatory requirements, and the identity industry. During Stage 4 maturity, businesses must focus on the goal of innovating and enhancing digital offerings with rich, differentiated, and up-to-date identity features — and they must do this seamlessly. This is a continuous journey that is unique for every organization, rather than an end-point destination.

### Our recommended steps and capabilities

In order to continuously optimize identity's impact within this stage, we recommend organizations implement the following customer identity solutions and capabilities:



#### Agility

- Full automation of identity and security policy management, user lifecycle management, and complex identity-related business workflows
- A centralized, intuitive admin UI with a unified view of all users
- Out-of-the-box integrations with best-of-breed third-party solutions related to fraud, risk, compliance, privacy, marketing, and others



## Experience

- Highly customizable and extensible customer access experiences
- Consistent, seamless, and personalized omni-channel experiences
- Deep integrations with the broader technology stack to create a single view of the customer organization-wide



## Security

- Intelligent MFA engine with the ability to ingest and analyze risk signals from a variety of sources
- Fully automated security workflows that support incident response and identity orchestration
- Risk-based, fine-grained authorization capabilities



## Reliability

- Resilient infrastructure that seamlessly and dynamically scales with demand spikes, including during unforeseen, highly trafficked events



## Strategy

- Fully-funded, multi-year identity program with executive buy-in
- Diverse internal stakeholder teams collaborating on identity strategy and program like a well-designed machine

Stage 1: Basic	Stage 2: Limited	Stage 3: Advanced	Stage 4: Strategic
<b>Goals &amp; challenges</b>			
<ul style="list-style-type: none"> <li>- Building and maintaining a nascent on-premises or homegrown service</li> <li>- Lack expertise and insight</li> <li>- Primarily concerned with onboarding customers</li> <li>- Basic capabilities</li> </ul>	<ul style="list-style-type: none"> <li>- More than one application or portal</li> <li>- Focus on creating differentiated and trustworthy customer experiences</li> <li>- Bolster internal operational efficiencies to support business growth</li> </ul>	<ul style="list-style-type: none"> <li>- Focus on streamlining the customer experience</li> <li>- Intelligent access policies</li> <li>- Integrated identity within technology stack</li> <li>- Consolidate data silos</li> <li>- Advanced automations and process efficiencies</li> </ul>	<ul style="list-style-type: none"> <li>- Mature omni-channel initiatives</li> <li>- Advanced features, integrations, and identity capabilities</li> <li>- Innovating</li> <li>- Enhancing digital offerings differentiated</li> <li>- Identity features seamlessly</li> </ul>

**Our recommended steps and capabilities for each maturity level**

<b>Agility</b>			
<ul style="list-style-type: none"> <li>- Basic user lifecycle management and policy management</li> </ul>	<ul style="list-style-type: none"> <li>- Partially automated user lifecycle management</li> <li>- Some / limited support: SAML, OIDC, a, FIDO</li> <li>- Some SDKs and APIs</li> </ul>	<ul style="list-style-type: none"> <li>- Advanced lifecycle management and automations</li> <li>- Some out-of-the-box integrations</li> <li>- Variety of SDKs and APIs</li> </ul>	<ul style="list-style-type: none"> <li>- Full automation of policy and user lifecycle management</li> <li>- Centralized admin UI</li> <li>- Out-of-the-box integrations</li> </ul>
<b>Experience</b>			
<ul style="list-style-type: none"> <li>- Single factor authentication with options for basic social authentication</li> <li>- Simple self-service functions (registration, password recovery, etc.)</li> </ul>	<ul style="list-style-type: none"> <li>- Limited SSO federation capabilities support for 3rd party identity providers</li> <li>- Extended social authentication options</li> <li>- Limited, partially customizable customer sign-in and registration experiences</li> </ul>	<ul style="list-style-type: none"> <li>- Automated account linking/merging</li> <li>- Advanced authentication customizations and logic</li> <li>- Progressive profiling</li> <li>- Passwordless</li> <li>- Identity proofing and account verification</li> </ul>	<ul style="list-style-type: none"> <li>- Highly customizable extensible authentication</li> <li>- Consistent, seamless and personalized omnichannel experience</li> <li>- Deep integrations within technology stack</li> </ul>
<b>Security</b>			
<ul style="list-style-type: none"> <li>- Basic security encryption and hashing</li> <li>- OIDC and OAuth 2.0</li> <li>- Basic access policies for APIs</li> </ul>	<ul style="list-style-type: none"> <li>- Basic MFA</li> <li>- Audit and monitoring tools</li> <li>- Integrations with standards-based API gateways</li> </ul>	<ul style="list-style-type: none"> <li>- Adaptive MFA</li> <li>- Risk detection and ttrack prevention</li> <li>- Some out-of-the-box security, privacy and compliance integrations</li> </ul>	<ul style="list-style-type: none"> <li>- Intelligent MFA able to analyze risk signals from a variety of sources</li> <li>- Fully automated security</li> <li>- Fine-grained authorization</li> </ul>
<b>Reliability</b>			
<ul style="list-style-type: none"> <li>- Limited high-availability</li> <li>- Limited failover and disaster recovery capabilities</li> </ul>	<ul style="list-style-type: none"> <li>- Plan for bursts/spikes often requiring ad-hoc investments and manual intervention</li> </ul>	<ul style="list-style-type: none"> <li>- Redundant servers, load balancers, and high-availability infrastructure</li> <li>- Service buffers to handle traffic spikes</li> </ul>	<ul style="list-style-type: none"> <li>- Infrastructure dynamically scales</li> </ul>
<b>Strategy</b>			
<ul style="list-style-type: none"> <li>- No holistic identity strategy, or strategies with disparate solutions</li> </ul>	<ul style="list-style-type: none"> <li>- Alignment and communication between diverse stakeholder teams</li> <li>- Evaluation of gaps and requirements to drive development investment plans</li> </ul>	<ul style="list-style-type: none"> <li>- Formal and ongoing processes for evaluating identity posture</li> <li>- Identity-related KPIs</li> <li>- Identity experts in-house</li> </ul>	<ul style="list-style-type: none"> <li>- Multi-year identity program with executive buy-in</li> <li>- Diverse stakeholder collaboration on identity strategy</li> </ul>



## Benefits of identity maturity

Following Okta's customer identity maturity model allows you to deliver new, superior digital experiences to your customers while unlocking several valuable business outcomes along the way, such as:

- **Increased identity effectiveness and ROI** with each stage of maturity unlocking more value than the last.
- **Operational and developer efficiencies**, thanks to intuitive, comprehensive tools for identity administrators and app developers.
- **Revenue acceleration via customer acquisitions and conversions.** Superior digital customer experiences turn identity into a business growth driver.
- **Enhanced brand trustworthiness** with the ability to mitigate security risks and recover promptly when incidents do occur.
- **A cohesive, forward-looking identity strategy** that accelerates value through more holistic, proactive planning.

# Unlocking customer identity's business value

Once you know where you're at in Okta's customer identity maturity journey, your organization can better assess next steps and monitor success. With clarity around new opportunities to innovate the digital customer experience, protect against security threats, and drive business growth — you'll be a step ahead of your competition.

In the next edition of this maturity guide, we'll share how maturing your customer identity posture will map to real business capabilities that generate value for your company.

As a proven customer identity partner, 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. Our customer identity solution grows along with your business and allows your teams to do their most meaningful work. To learn more about how Okta can get you on the path to customer identity maturity, visit [okta.com/customer-identity](https://okta.com/customer-identity).

---

## About Okta

Lorem ipsum dolor sit amet, verear dolorum dissentias pri te. Eam te discere bonorum tractatos, ne vix mutat legere aliquip, per no paulo accommodare suscipiantur. Ei quo meis ubique delicatissimi. His paulo noluisse ei, legere molestie ne sea. Quo menandri sensibus ne, te legimus epicuri vis. Id facete accusam molestie cum, at graeci dictas consequuntur est. Unum omnis delectus qui cu. Nibh copiosae id vis. Has aliquam inermis nonumes at. Dicta erroribus voluptatum et sit, mazim dolore ei usu, in alterum euripidis concludaturque eam. Id quot adversarium cum, pri ea meliore inermis consequat, vis impetus tritani ex. Mea cu ludus. To learn more, visit [okta.com](https://okta.com).

