okta

From Zero to Hero:

The Path to CIAM Maturity

Your guide to the CIAM journey

As the leader in identity and access management (IAM), Okta has worked with thousands of companies to achieve their security and usability goals. We've learned that no matter how far along each company is on their identity journey, there's a common set of challenges they face at every step.

In this eBook, we define and discuss four key phases on the path to customer identity and access management (CIAM) maturity and the pain points that companies encounter in each phase of the maturity curve. We propose solutions for each of these problems, providing a roadmap for the tools and processes you should adopt as your organization moves ahead.

Wherever you are on your journey, we offer clear next steps to take on the road to continuous customer identity and access management. Let's get to it.

Mapping the way to CIAM maturity

What is customer identity and access management (CIAM)?

The challenge: providing the level of digital convenience customers expect while keeping them secure. The solution: let go of outdated approaches to IAM and replace them with modern technologies that protect user identities and ensure the right people have access to the right resources—for the right amount of time. That's CIAM.

Building identity features in-house is a complex and time-consuming task—if done incorrectly, it can trigger a number of security vulnerabilities. Many organizations struggle to scale their apps and bring them to market at a competitive pace. In a landscape where security breaches and data misuse cases are frequent news items, customers are losing confidence in digital experiences and the companies collecting their data. As such, efficiency and user trust are the new currency for companies looking to scale.

To reduce the development time of digital properties, eliminate security gaps, and provide seamless user experiences, businesses need to put their customers' identities front and center.

CIAM solutions embed an identity layer into customer-facing apps and portals, safeguarding data and user accounts, and facilitating easy and secure access to websites and apps. They are the foundation that enable organizations to effectively meet their security, privacy, and marketing needs.

The three main features of an effective CIAM solution are **authentication, authorization, and user management**. These components will evolve across your journey.

What is **authentication?**

Proper authentication ensures that the people logging into their accounts are who they say they are, preventing bad actors from accessing sensitive user data (e.g., payment details, address, SSN).

What is **authorization?**

Effective authorization helps businesses confirm that a user has the right level of access to an application and/or resources.

What is **user management?**

Clear user management allows admins to update user access permissions and implement security policies, better enabling seamless and secure experiences.

CIAM architectural scenarios

CIAM supports organizations in a variety of operational contexts, including:

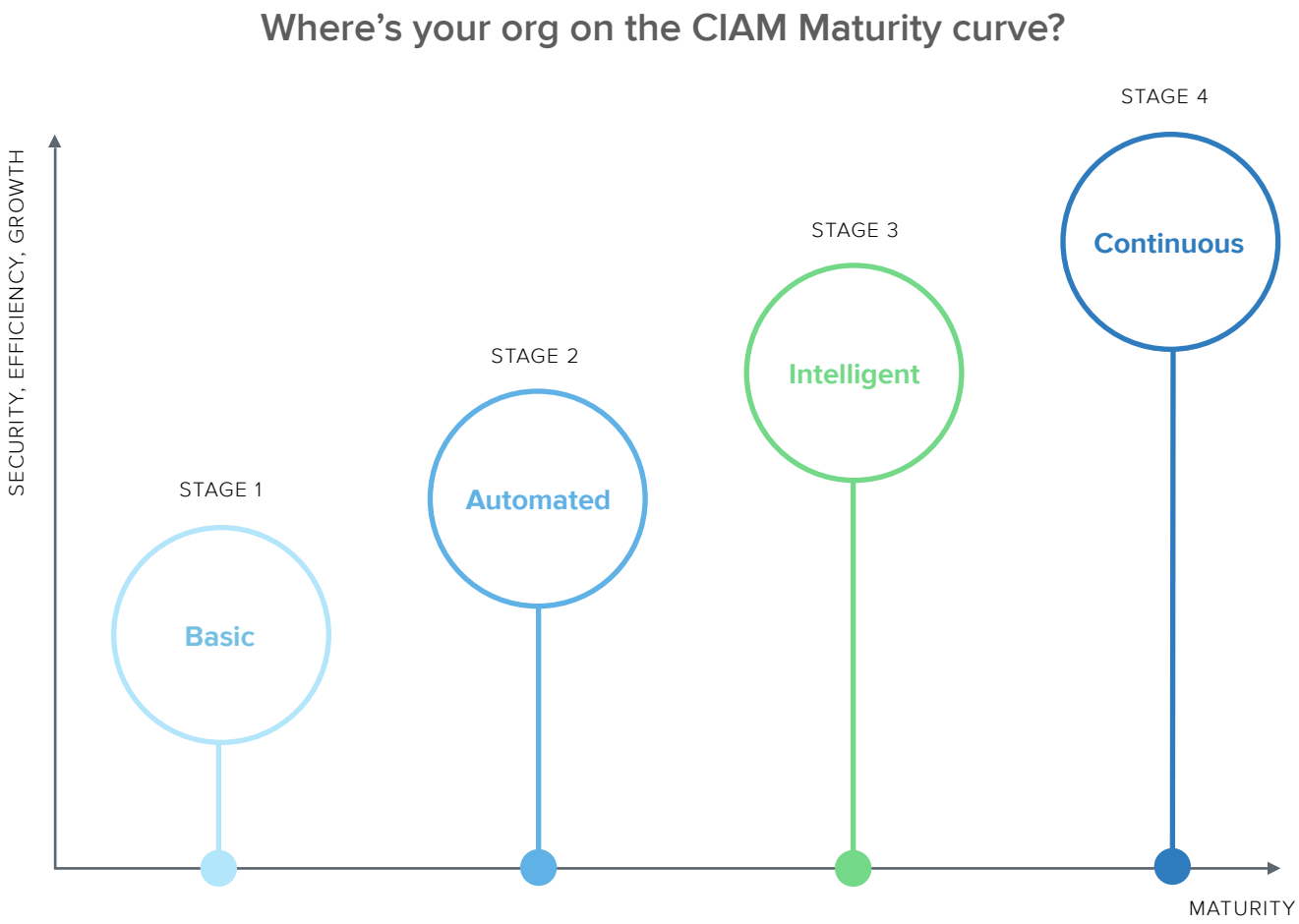
- Business to consumer IAM
- Business to business IAM
- Single sign-on for regular web apps
- SPA and API
- Mobile and API

Whichever scenario applies to your organization, you'll have several steps to take as you launch your customer-facing product. This includes building apps, securing APIs, protecting users, and integrating enterprise identities.

In every instance, implementing robust CIAM infrastructure will protect your customers' data and secure their access, inspiring trust in your products.

The CIAM maturity curve

Naturally, different organizations are at different stages of maturity when it comes to CIAM. We define these four stages as: **Basic, Automated, Intelligent, and Continuous.**



Let's take a closer look at each stage and the steps you can take to move your company forward on the path to CIAM maturity.

Stage 1: Basic

Prove your product/market fit

At this stage:

- ✓ You have a great product idea and want to demonstrate its viability.
- ✓ You're at the start of your project.
- ✓ Your team is small:
  - Nearly all of its members are tasked with the application launch.
  - You have one to two technical leads with breadth of experience.
  - There's no dedicated identity expert.
- ✓ Your project is early in its lifecycle, likely pre-revenue with early access prospects.
- ✓ The team's core focus is to design, build, and validate the application's business hypothesis.

Stage 1 goals and challenges:

Goals

- Your goal is speed-to-market: quickly ship an early minimum viable product to which basic identity is a prerequisite.
- You want to get your product in front of potential customers.
- You are focused on proving you are solving the right problem.

Challenges

- You have to ship your product.
- You have to iterate as you learn more.
- You have to establish a set of KPIs for your product and gather feedback in a short timeframe.
- Basic security issues could derail the project.
- You have limited engineering resources and lack insight into where identity fits into your design.

Build vs. buy

At this point, it's common for companies to decide whether they want to spend time and resources on building their own CIAM solutions or partner with a third-party provider. Building and managing tools internally can take up valuable time from your developers. Taking advantage of an external solution can keep companies agile: your teams will have the time and resources to continue enhancing your product without the distractions of maintaining an unwieldy internal CIAM system.

Needs

Your CIAM solution needs to support the quick setup and integration of:

- User sign-up and onboarding.
- User sign-in.
- User access rights.
- User authorization.
- User management.
- Password reset and account recovery flows.

Solutions

Core CIAM platform components

As mentioned in our introduction, the three main features of an effective CIAM solution are:

- Authentication (sign-in).
- User management (sign-up).
- Authorization (access rules, policies).

Customizable user flows

Predefined and customizable user flows can quickly deliver best-in-class user and customer support functions:

- Self-serve registration
- Password reset
- Account and username recovery

Credential recovery

Your credential recovery should include a knowledge check (e.g., security question) and a basic possession check (e.g., email link reset).

Your credential recovery mechanism needs to support a side channel—like email recovery—to let the user reset their password.

The credential recovery mechanism should only support one-time and/or limited-time use.

Developer efficiency

On average, developers spend 17.3 hours a week debugging and maintaining legacy and bad code. The right CIAM platform can speed up development and reduce the pain of maintenance later. Now, you can focus on core customer and product experiences, and your teams can easily build production-ready identity integrations with the best available tools.

Your CIAM solution should enable security policies to be maintained and updated without getting your engineers involved.

Centralized identity management

This provides security and admin teams with the ability to manage security policies without the need for code, and the ability to apply a consistent framework as you scale.

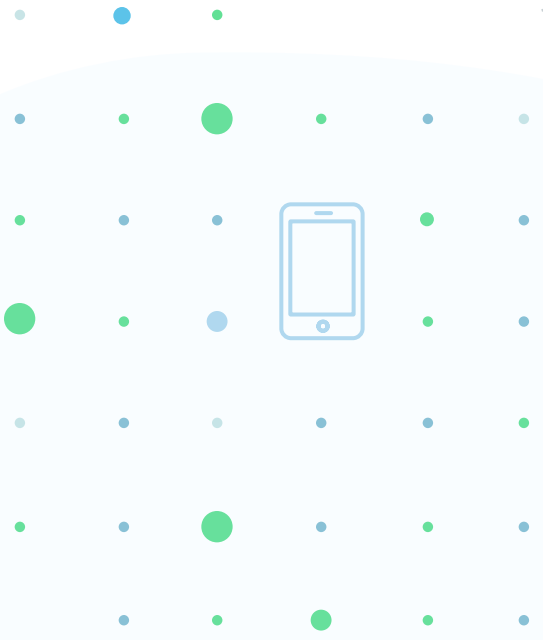
Your CIAM solution must adhere to basic security best practices and modern identity standards.

Security

This includes:

- Encryption and hashing.
- Open identity standards like OIDC/OAuth.
- Adopting platforms like Okta, which is a leading authority in defining security specs.

A modern CIAM platform can securely store user credentials and mitigate broken authentication flows, which are the second most prevalent web application security risk.



1 Graduating from stage 1 of the CIAM maturity roadmap

Authentication

- Authentication standards
- Social authentication
- Password reset flows

Authorization

- Authorization standards based on OIDC and/or OAuth
- Authorization server

User management

- Simplified onboarding
- Self-service registration
- Streamlined admin

Centralized admin UI

- Access policies
- Security policies
- Consistent implementation

Developer experience

- Tools: SDKs, APIs, widgets
- Documentation: guides, sample apps
- Integrations across the developer ecosystem

To learn how you can implement these features with Okta, watch our Customer Identity demo.

Achieving basic CIAM maturity means you've built crucial identity security features into your app—and you've successfully brought it to market. Next, it's time to think about expanding your product offering to serve a growing customer base.

2 Stage 2

Stage 2: Automated

Centralize and scale

At this stage:

- Your application was a hit and you're now looking to build additional products for your customers.
- Your team is growing: you've hired a number of additional developers, technical managers, and product managers.
- You have a CTO, VP of Product, or VP of Engineering leading your project.
- You have a growing paying customer base that demands more advanced or enterprise-grade features, which you might not have the time or experience to build.
- While you need to prioritize your own initiatives, customers want you to develop more sophisticated identity capabilities and integrations.
- Your leadership and company goals are aligned on scaling your organization and products, and developing efficiencies for sustainable long-term growth.

Stage 2 goals and challenges:

Goals

- You need to decide if identity is critical enough to build the capability in-house.
- You've launched two or more product areas and are looking to translate the success of your previous product into another.
- You need to have the loyal fans of your first product adopt your second product.

Challenges

- Your organization needs to meet various compliance requirements, like the GDPR and CCPA.
- Your team may not have the required experience and expertise in the protocols, standards, integrations, and operational challenges of identity systems.

Needs

Your CIAM solution needs to help you offload the risk and management of external identities:

- End users should be able to sign in with existing identity providers.
- You should be able to delegate authentication to existing LDAP or Active Directory.

Your CIAM solution should provide modern standards and allow you to pick the best approaches and security practices without constantly playing catch-up.

Solutions

Scaling user management

The right CIAM solution gives you the ability to federate users into your application with their existing identities.

Connect your customers' or partners' LDAP or Active Directory to synchronize user accounts to your existing user store and offload the risk of managing those identities.

Standards and future-proofing

Your CIAM solution should support modern authentication standards such as OpenID Connect, OAuth, and SAML and constantly align to latest specs.

- Adopting the latest standards via automation is extremely important as you scale.

Security and identity standards are regularly changing. You'll want to track:

- Standards and protocols
  - JWT
  - SAML
  - OAuth2.0/OIDC
  - FIDO
  - PKCE
- Identity providers
  - Sign-in with Apple
  - Social Auth

Your CIAM solution needs to automate processes like provisioning and deprovisioning while managing data privacy.

Automated provisioning with lifecycle management

The right CIAM platform will offer automated workflows tied to where your customers are in their lifecycle.

- This way, you can provision and deprovision users to downstream applications and systems across your stack.

Your CIAM solution needs to strengthen security as you scale and become a larger target:

- It should automatically flag insecure or compromised passwords.

This needs to be automated without using developer resources.

Password security

Modern identity systems allow admins to:

- Specify password complexity.
- Check for common passwords.
- Check for compromised passwords.

Your CIAM solution must protect one of the most vulnerable points in the user journey: account or password reset flows.

Meet the needs of your growing customer base

Modern solutions support secure password reset flows that leverage a strong level of assurance to reset credentials. It supports:

- Security questions.
- SMS.
- Voice.
- One-time passwords to reset your password.

Your CIAM solution must allow you to easily increase security in your app, with minimal friction to end users. It should:

- Protect against account takeover.
- Offer assurance levels and ensure the user has possession of the token.

Protect users with MFA

You need to choose and implement authentication factors that are appropriate for your customers and use cases. This may include factors that ensure proof of possession, cryptographic security, and common channels like SMS, Google Auth, email, etc.

Explore the various types of authentication assurance levels.

Your CIAM solution should be extensible and allow for customized authentication logic.

Extended platform functionality with hooks

Your CIAM solutions should allow you to extend core platform processes like authentication in order to perform actions such as:

- Registration, user import, and authentication.

Your solution should cover the underlying APIs that power your applications, whether they're for internal or external users.

API access management

API access management provides granular control for access to application backends and other backend processes using Oauth2 client credentials grant flow.

API access policies and access grants should be configured in the CIAM solution's dashboard.

2 Graduating from stage 2 of the CIAM maturity roadmap

Authentication

- SSO
- Password policies
- Secure reset flows

MFA

- Basic level factors: SMS, email, Google Authenticator

Authorization

- API access management and API access policies
- Integration with API gateway for consistent view of user authorization

User management

- Single source of truth, attribute level mastering, user profiles
- Multiple profiles for one identity
- User mastery

Advanced inbound federation

- Generic OIDC
- SAML
- Single user profile (aggregating)
- Single view of users
- Account reconciliation

To implement these features with Okta, get started now with our free developer plan.

With this stage completed, you've expanded your product reach and increased the sophistication of your user management, compliance, and security capabilities. As you continue to scale, you'll want to invest in stronger security protections and new customer experience features.

3 Stage 3

Stage 3: Intelligent

Optimize without compromise

At this stage:

- ✓ You are in a position to lead the market with your product.
- ✓ Complex stakeholders (e.g., product, engineering, and marketing teams) all have specific identity requirements.
- ✓ You want to optimize your offering while also:
  - Scaling and establishing a deep market presence.
  - Retaining a competitive advantage.
  - Keeping your users and applications secure.
  - Preserving the development teams you have across the organization.

Stage 3 goals and challenges:

Goals

- You need to protect the company's data, infrastructure, and users.
- You need to streamline the customer experience, removing friction and applying new features via personalization and analytics.
- You need to connect the product lifecycle to the marketing engine and focus on branding and analytics.

Challenges

- Each team has different priorities and trade-offs that you need to balance while still delivering useful things for customers.
- You're having to continually improve your infrastructure to use microservices and APIs to ensure your systems are modular and secure.

Needs

Your CIAM solution needs to add a higher level of assurance to your registration experience.

- End users should be able to sign in with existing identity providers.
- You should be able to delegate authentication to existing LDAP or Active Directory.

Solutions

Sophisticated onboarding

The right CIAM solution will include identity proofing and account verification to validate only legitimate users and onboard them onto your platform.

- The registration process validates the user and ties them to a real physical identity.

The right CIAM processes will also help you pass from identity resolution to identity validation.

Your CIAM solution should be highly secure and seamless, facilitating accessible and trustworthy user experiences.

Adaptive MFA

This solution offers an adaptive intelligence layer that uses biometrics (e.g., TouchID, FaceID) and behavioral inputs to assign risk and additional authentication when needed.

Your CIAM solution should allow you to reliably identify and mitigate security risks.

Platform data

Leveraging Okta's platform, for instance, brings more event and activity data under your scope, leading to proactive risk detection and attack prevention.

Your identity strategy should incorporate a central system that stores and links together customer data, with automated policies in place to fulfill compliance requirements.

Privacy and compliance

You can consolidate user lifecycle and data management in a central connective system for easy deletion, updates, and downloads to meet privacy and security compliance requirements.

Your CIAM solution needs strong authenticators that allow you to move beyond passwords.

Passwordless authentication

Passwordless technology using email magic links or WebAuthn allows you to eliminate all identity attacks caused by stolen or compromised passwords.

Your CIAM solution should enable your security stack to work in unison by providing in-depth security.

Security extensibility

Security products such as bot mitigation solutions and web application firewalls work in conjunction with your CIAM solution to stop all attacks.

Your CIAM solution should create user convenience along the customer journey.

Optimizing for minimal friction

Progressive profiling lets you build custom experiences that capture user attributes over time, lessening friction.

Your CIAM solution needs to be extensible and allow for customized authentication logic.

Platform extensibility

Your CIAM solutions should support extensibility with features such as hooks. These extension points should be incorporated along the user journey at stages like registration, user import, and authentication.

Your solution needs to meet each stakeholder's specific needs.

Integration

Okta's integrations connect all the pieces of a user's identity, allowing you to choose the best system for each situation (e.g., ticketing/support, CRM, ecommerce platform).

Your CIAM solution should work with leading privacy and compliance vendors.

Okta at the center of your stack

Your CIAM solution should map data attributes and seamless sync changes across the different elements in your identity, marketing, and preference tools. Modern CIAM solutions can integrate with privacy tools that track customer preferences and privacy compliance requirements.

3 Graduating from stage 3 of the CIAM maturity roadmap

Authentication

- Passwordless authentication

MFA

- Adaptive authentication

User management

- Registration hooks
- Progressive profiling

Customization

- Hooks
- Personalization

Integrations

- ID proofing integration
- Fraud and risk integration
- Security integrations
- Consent and privacy integration

To learn more about how Okta can help, check out the following resources:

- Adaptive Multi-Factor Authentication
- Passwordless Authentication Platform
- Okta Hooks

At this point, your application provides customers with strong, perhaps even passwordless protection. Your use and storage of customer data gives rise to personalized quality-of-life improvements and is fully compliant with data privacy regulations. Thanks to industry-leading integrations, your identity security is stringent and you can proactively detect and mitigate risks. Customers use your services with trust and ease, and you're well-positioned to explore advanced functionalities.

4 Stage 4

Stage 4: Continuous

Lead and set the new standard

At this stage:

- Your product is a clear market leader.
- There's strong alignment on your digital transformation project.
- You have an omni-channel strategy that optimizes for both security and user experience.
- Your product has robust integration with advanced fraud and risk solutions.
- You view identity as a continuous journey with a long-term strategy.
- You have identity experts in-house and a director of CIAM.

Stage 4 goals:

Goals

Security

- You want your users to authenticate when appropriate.
- You want to automate your security response and orchestration.
- You want to reduce the number of security policies/rules in place.

Omni-channel experience

- You want to track your users across different channels such as store, mobile, and web. You aim to support and unify the customer journey and experience.
- You want to reduce fraud across channels.

Fine-grained authorization and risk-based authorization

- You need dynamic authorization based on the risk and context of the user.

Compliance

- You need privacy by design, with data processing and storage practices that align with evolving regulations.

Needs

Solutions

Your users expect long session times, and you want to make these session times as frictionless as possible.

→

Useful risk signals

Your CIAM platform needs to ingest and analyze risk signals from a variety of sensors to determine session risks.

Sensors can be a combination of both internal and third-party risk signals. Risk signals can be set for categories like:

- Network
- Location
- Device
- Transaction

When the risk score is above a specific threshold, your CIAM platform can force the user to revalidate their identity or end the session.

The session risk score computation can be scheduled at fixed time intervals or triggered by specific user events in the app.

You want to automate your security response and orchestration.

→

Flexible security workflows

Security workflows that support incident response and identity orchestration will encourage incident enrichment and coordination.

You want to reduce the time and effort spent to manage identity and security policies.

→

Reduction in security policies

The AI/ML capability of your CIAM solution will reduce the number of security policies that your admins need to manage.

You want to track your users across channels and offer a seamless experience between each channel.

Omni-channel user experience

All user engagement channels should authenticate or store authentication data with your CIAM solution.

All digital channels should authenticate over standard protocols to provide a single view of the user.

Okta's security information and event management (SIEM) app and dashboard can show log aggregation from Okta and third party omni-channel authentication tools.

You want granular control over any data exposure.

Regulations and controls

Risk-based authorization determines who can access particular data elements and where data is accessible from.

It also provides support for granular access control to applications and data sources or types.

You likely need to support Open Banking specifications and strong customer authentication (SCA) transaction signing.

Meeting industry standards

Financial-grade API (FAPI) support for read/write transactions should be supported by your CIAM solution's authorization engine.

SCA transaction signing should be supported by existing factors.

4 Embracing stage 4 of the CIAM maturity roadmap

MFA

- Continuous authentication
- Third-party risk signals
- Multi-model AI risk engine
- Security and identity orchestration and response

Authorization

- Fine-grained authorization

Standards

- FAPI
- SCA

Integration

- Omni-channel authentication integration

To learn more about how Okta can help, check out the following resources:

- Risk-Based Authentication: Because You Shouldn't have to Choose Between Security and Usability
- Okta Insights
- Okta + PlainID

CIAM Maturity

No more roadblocks on the path to CIAM maturity

Whether you're a first-time product developer or an established market leader, embedding CIAM into your product roadmap is crucial. Knowing your stage on the CIAM maturity curve means that your organization can monitor successes and identify focus areas—clarity that gives you a competitive advantage.

Building the best possible app or digital service requires a focused and empowered pit crew. With Okta as your CIAM partner, you can dedicate time and resources to what you do best while we monitor regulations and build integrations. Our CIAM solution grows along with you, freeing your developers to do their most meaningful work.

Get in touch to see how Okta can get you on the path to CIAM maturity.