Brought to you by:

IBM Security

Consumer IAM (CIAM)

for dummies®
A Wiley Brand

Understand the CIAM landscape and benefits

Plan your CIAM strategy and use cases

Consider functional deployment factors

Martijn Loderus

IBM Security Limited Edition

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development, and delivery organizations. Monitoring more than two trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit **ibm.com/security.**

Consumer IAM (CIAM)

IBM Security Limited Edition

by Martijn Loderus

for dummies®
A Wiley Brand

Consumer IAM (CIAM) For Dummies®, IBM Security Limited Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-119-71560-3 (pbk); ISBN: 978-1-119-71562-7 (ebk).

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Manager: Carrie Burchfield-Leighton

Sr. Managing Editor: Rev Mengle

Executive Editor: Steve Hayes

Contributing Author: Jack A. Hyman

Business Development Representative: Molly Daugherty

IBM Contributors and Partners: Anna Fernezian, Marc von Mandel, Rich Edwards, IBM Security Verify, Akamai, Okta

Table of Contents

Introduction

Global organizations want to achieve the right balance of convenience and security in protecting their consumer-centered users. Security policy decisions, especially those for consumer-facing services, challenge the marketing and product leaders and can create friction. A low-friction login experience is a must because, unlike employee use cases, consumers will abandon an application or web-based login experience because they have alternatives. Building a trusted relationship between consumer and brand means building predictable experiences across omnichannel platforms (web, mobile, and social) for your brand. From an operational perspective, this includes attributes such as authentication standards, performance management, system scalability, user-experience management, systems integration, and analytics. All these features will be an integral part of a Consumer Identity and Access Management (CIAM) solution.

Enterprise Identity and Access Management (IAM) systems are designed to give access to business applications and services inside corporations such as an intranet or portal. The user is part of a trusted relationship established by Human Resources (HR) and isn't expected or required to have credentials through any third-party vendor platform. This trusted relationship isn't assumed for consumer-facing applications. CIAM engagements must be accessible and designed for zero trust because every interaction can be hostile.

CIAM is mainly a Software-as-a-Service (SaaS)-based solution offering many intrinsic benefits: It allows organizations to provide self-service registration and profile management capabilities, offers single sign-on across multiple websites, and ensures privacy and consent are effectively captured and managed. Developers can build their experiences where identity management is integrated based on API-friendly development kits. IT leaders can monitor and manage authentication and authorization processes in real time using robust analytics and insights. Another advantage is CIAM's highly configurable regulatory and compliance controls in support of data privacy regulation. These features are critical to ensure backend systems can only use the data when consented, ensuring the consumer data is safe, secure, and authorized, supporting the organization's channel engagements at all times.

About This Book

Consumer IAM (CIAM) For Dummies, IBM Security Limited Edition, emphasizes what CIAM entails and how it benefits organizations. This book also offers practical suggestions you can use when your organization decides to implement the technology. You find out about the use cases and user personas involved in implementing CIAM to better understand the consumer context from a business perspective.

This book takes a vendor-neutral approach to technology. I provide you with building blocks as an executive or technical professional to design and develop a robust CIAM solution applying industry best practices.

Icons Used in This Book

Throughout the book, you find icons that point out things that are important about CIAM. These are brief concepts. If you see one of these icons, simply take note.

TIP

Look at the Tip icons because these are indicative of important takeaways.

REMEMBER

When you see this icon, you may find the information useful. This information relates to details or experiences that provide context to the topic at hand.

WARNING

Warnings are subtle alerts! I use alerts in the text to inform you of common errors and mistakes that you should avoid.

Beyond the Book

Unfortunately, this short book can't share the depth needed to formally implement a CIAM solution, so for additional resources to guide you, visit `www.ibm.com/security/digital-assets/iam/consumer-identity-and-access-management`.

IN THIS CHAPTER

- Understanding the fundamentals of CIAM
- Seeing the difference between IAM and CIAM
- Identifying the key business functions of CIAM
- Following the evolution of CIAM
- Appreciating CIAM as a consumer-facing identity provider
- Using CIAM with digital transformation
- Looking at deployment models
- Justifying why CIAM makes business sense

Chapter 1
Surveying the CIAM Landscape

Consumer Identity and Access Management (CIAM) synthesizes the relationship between the consumer and brand. Consumers require a platform that supports features such as self-registration, a system to support authentication, and a method to collect consent for data usage in enterprise data systems and devices. CIAM enables a personalized and secure interaction for you to safely shop, play online games, or control your home devices.

In this chapter, you discover more about the business drivers, technology, and capabilities used to protect consumers in numerous environments that make CIAM an attractive option for an enterprise organization.

Introducing CIAM

CIAM solutions are mostly Software-as-a-Service (SaaS)-based cloud solutions. The CIAM solution that IT organizations utilize encases a single identity management system specially tailored toward consumer engagements, so reliability needs to be treated as business critical.

Because both Identity and Access Management (IAM) and CIAM support identity engagements, it's important to highlight some major differences. Three differentiators between workforce IAM and CIAM include

- **Access for one versus many:** IAM solutions are designed to support access for the right person at the right time for the right reasons. You can think about this as giving access to a vault where you need to have the right access code to open it. CIAM solutions have a totally different objective. They want to give access to as many people as possible, but when authenticating, you want to capture users' identities to engage with them in a personal manner. Envision an entrance of an amusement park where many people want to enter. While entering, you get their names and details to ensure you can sell and market to them.
- **Supporting self-service engagements:** CIAM solutions are mostly in support of marketing campaigns or e-commerce use cases where the customer self-registers for his product or service purchase. In IAM use cases, the individual is usually provisioned by Human Resources (HR) or the IT department based on a trusted relationship the user has with the employee or partner.
- **Scale and impact:** IAM solutions are supporting companies and their employees to provide access to systems and services. This means IAM supports tens to hundreds of thousands of users. As CIAM is supporting the relationship between consumers and brands, these engagements support hundreds of millions of customers who are buying their latest products or services. CIAM can directly affect revenue and the impact on brand loyalty and image.

Figure 1-1 shows you a typical CIAM outline across various customer-facing websites and apps, potential social identity providers (IDPs), and back-end systems with controlled access to customer data for personalized engagements.

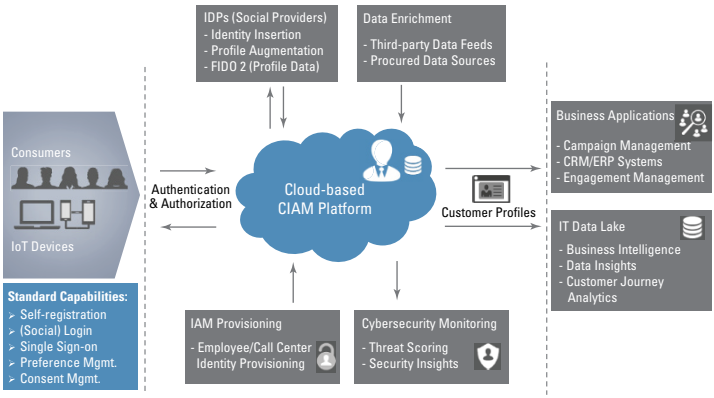

FIGURE 1-1: A typical CIAM implementation.

Because business applications and data stores can utilize the consumer data attributes from a centralized source, the CIAM solution becomes a formidable option to securely engage with consumers and build a trust relationship no matter what communication channel they're utilizing.

Understanding Why CIAM Is Not IAM

CIAM approaches security by using an omnichannel approach. When users sign themselves up for a website, mobile platform, or Internet of Things (IoT) application, they create their own profiles in the context of their personal objectives — like getting a coupon or shopping online. Employees' identities are managed by the corporate entity using traditional IAM tools where HR or the IT department provisions user privileges in the corporate setting.

Authentication is another reason why CIAM isn't like IAM. With CIAM, public standards, such as OpenID, allow social login aggregators to validate end-user identities with already-established identities. The user can also create multiple accounts or personas on a single platform. In the corporate environment, a user has a unique account that maps to an internal service directory. The user is a known, captive entity. Trust can be assumed in the corporate setting, but in the consumer environment, trust isn't assumed and needs to be earned over time.

Performance management is another differentiator between CIAM and IAM. The consumer is less tolerant of lackluster system performance. Because users have alternative choices, their thresholds for poor performance are low. At the corporate level, users deal with system latency, poor user experience, and network degradation because they have no other options to execute on their tasks.

System scalability varies considerably between CIAM and IAM. For consumers, a small system can contain as few as a million users to as many as hundreds of millions of active users. A corporate system leveraging traditional IAM will typically support tens to hundreds of thousands of concurrent users.

IT systems operate on various internal and external networks for different purposes. In the context of CIAM, system IDPs use public connections for decentralization. The same isn't valid for corporate systems because they often leverage a single IDP.

Unlike IAM, you can't expect a user to utilize complex security mechanisms. For example, with enterprise IAM, employees or corporate users may be expected to use multifactor authentication (MFA). With such a use case, the population is finite. Using such tools is considered acceptable. However, with CIAM, users sign up for new security credentials all the time. If a vendor creates a complex user experience, the users will abandon your product.

Finally, customer data collection is process-driven in the context of CIAM. Activities such as transactions, marketing personalization, and business intelligence are inclusive of such collection practices. Additionally, customers are often subject to a large number of privacy and data protection regulations, depending on their region. Corporations are more concerned about internal administrative and operational actions in addition to globally centered policies.

Looking at the Business Functions of CIAM

Business requirements often drive technology decision making. When certain features are expected to be a part of an enterprise's operations, it becomes a requirement. Business requirements can

be technical, functional, or even policy based. The key business drivers of CIAM focus on

- **User conversion:** The end-user experience should be fluid across all channels, including web, mobile, and social. There's a fine balance between security and the friction impact of the experience. The developer should be able to build new applications securely by using Application Programmable Interfaces (APIs) that are easy to deploy and that keep great user experiences in mind.
- **Security:** Applications should utilize single sign-on, multifactor authentication (MFA), or implement self-service and user management with easy-to-consume REST APIs to support common actions, including enrollment, registration, and other identity operations.
- **Data protection and privacy:** Adherence to data privacy regulations, such as General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), is essential with a clear and transparent user-consent function. Tracking privacy and consent preferences can give users control over their data.
- **Performance management:** Applying analytics to monitor the performance of systems, whether it's application usage, transaction management, or token usage, improves the consumer experience and delivers risk management.
- **Identity integrations:** Leverage a single platform for login capabilities across all channels by using streamlined authentication connectors, such as OAuth2, OpenID Connect, and Security Assertion Markup Language (SAML) 2.0, to support one application login for ease of use.

The Evolution of CIAM

For several decades, most organizations have made IT investments exclusively on enterprise-centric IAM. Most recently, however, a shift has occurred due to the consumer influence in today's corporate operations and digital transformation efforts.

Starting with the notion of Bring Your Own Identity (BYOID), the concept of (social) login IDP services was born in early 2000. This

birth allowed people to skip registration forms and register with an already established identity. Today, most CIAM vendors support many IDPs to allow for lower friction during registration or login activities. In this decade, more banks, healthcare providers, and governments are expected to embrace the concepts of decentralized identities to provide their services.

While most enterprise IT organizations have some level of centralized IAM services to support customer-facing services for their employees, these services are often attached to existing or legacy enterprise-IAM platforms. To date, this has been the status quo, but customers and line of business leadership demand more. New services and engagement models are designed with customer identities at the center for the digitalization of business models. As a result, the need to establish a service-based CIAM platform is clear.

Supporting Modern Consumer Needs

The consumer is being empowered by more and more global initiatives of governments who are defining data subject rights. This means that next to a great experience, the access and ownership of consumers' data needs to be respected and can't be used without their consent.

How is this changing businesses and the functional requirements? To answer that, you have to look at different angles to understand the real impact of this consumer empowerment:

TIP

- **Be unique and relevant.** Marketing is the driver to engage the consumer, and IT needs to support the transitions from user experiences to logins and authentications in a streamlined fashion.
- **Provide low friction.** Conversion rates are predicated on the level of friction that the user experiences. Using federated identities, having adaptive authentication methods, and providing clear interactive engagements are essential.
- **Provide a secure, seamless, and unified customer experience.** An omnichannel experience to protect consumers should be provided. Consumers will engage from a web browser, a mobile app, or through a connected tool to respond to brands. The same user login and data access experience can deliver brand loyalty.

- **Support the consumer.** Support should come across any interface as a means to simplify logins and build trust and brand awareness.
- **Be highly scalable.** Due to the unpredictable success of your campaigns, you'll have unpredictable loads. Focus on scaling your system for large public audiences. The user base isn't usually tens to thousands; it's generally millions or more.
- **Provide self-service.** Allow users to complete the activities on their own. Make it intuitive and user friendly. Strong user experience is essential.
- **Offer privacy, consent, and preference.** Always ensure the user is aware of who's in control and how her data is being used. Make sure to provide the controls to manage her data.
- **Allow for modular integrations.** Allow for the integration of social, mobile, API/software development kits (SDK), and enterprise systems using a consistent, repeatable process.
- **Be reporting- and analytics-centric.** Focus on creating a quality relationship based on personally identifiable information (PII) and metadata outputs.

Supporting Digital Transformation

The consumer has a growing expectation for contextual, personalized experiences. The end-user expects that the online experience, regardless of platform, is flawless, predictable, and consistent. To ensure that the consumer experience is delightful, organizations continually transform their operations to meet the needs of the digital economy.

REMEMBER

To meet these demands, during the implementation of a CIAM system, both the marketing and technical teams must consider the following factors:

- **Economic disruptors:** Customers expect that organizations remain innovative and technically adapt to today's customers' needs. There's often a blur between personal and business needs.
- **IoT:** Almost every solution has become data-rich and includes a digital component, sensor, app, or ancillary app.

- **Cybersecurity concerns:** Overreach and security concerns given deficient identity and data management practices remain a top concern.
- **Perception:** Public perception of data collection practices has led to defensive behavior and a stronger desire for consumers to want more control over their data.
- **Regulatory changes:** Because the consumer is becoming more aware of how his data is collected, used, and accessed, more regulatory controls are being put in place by governments to ensure protection, transparency, privacy, and power.
- **Demographics:** The consumer is rapidly evolving. Younger users (Generation Y and Z, for example) are more actively using the Internet to conduct transactions almost exclusively for commerce-centric activities. The desire to protect and secure your identity directly ties to the use and adoption of a well-built CIAM platform.

Identifying Deployment Models

Consumer applications, interfaces, and login credentials, no matter how one accesses them, influence the consumer experience. Resources within the enterprise data center support traditional IAM as part of an on-premises hosting environment. When resources shift from a data center to the cloud, this is considered an off-premises solution. CIAM is mostly considered a cloud-based solution due to the unpredictable loads and availability requirements.

Off-premises infrastructure, such as cloud compute capabilities, often reduces the IT internal labor and resources footprint. The design of the infrastructure doesn't fit a cookie-cutter model for all organizations. As described by the National Institute of Standards and Technology (NIST), when deploying a CIAM solution, an organization may use four specific cloud infrastructure deployment models:

- **Private clouds:** Considered the most secure deployment model, this support model is used almost exclusively for single private organizations or internal customer instances.

- **Public clouds:** Commonly used by independent organizations that share space, this deployment model is popular in the deployment of SaaS applications.
- **Community clouds:** When there's a common purpose, mission, or audience, this model is often the preferred architecture.
- **Hybrid cloud:** This model is a combination of two or more of these models in support of an organization's application or data storage needs.

REMEMBER

CIAM services can be deployed as centrally hosted, via APIs, or in combination with other access management tools, often across one or more cloud environments. CIAM platforms allow an enterprise organization to deliver a trusted identity with a frictionless user experience that balances security and convenience.

Making Business Sense of CIAM

Consumers expect their online experiences to be fluid, whether they're seeking information or committing a transaction. When it comes to entering and maintaining security, the user mandates a seamless experience. Such behavior is especially true for those who are well-versed with online interactions because they prefer self-control and personal engagement.

The modern organization can support security engagements by reducing cyber threats, increasing omnichannel interaction and flexibility, and reducing cost through the use of CIAM. The four key business distinctions that justify why CIAM makes business sense include the following:

- **Increases loyalty and trust:** Deliver a streamlined, omnichannel experience that protects customer data regardless of format.
- **Streamlines access:** CIAM allows the customer to access sign-on options and register how she feels comfortable by using balanced security approaches.

- **Multichannel personalization:** Deliver anywhere, anytime consistent personalized experiences no matter how the customer interacts with the brand via any device.
- **Security and privacy:** CIAM protects the customer from fraud, breaches, and cyber threats through enforcement and privacy mandates.

Consumer identity isn't an easy task to tackle. Data needs must be evaluated from both the back and front ends, across various system integration points. CIAM platforms offer an affordable modular approach to handling identity experiences in the enterprise by using secure and low-friction capabilities.

IN THIS CHAPTER

- Allowing for centralized consumer profile management
- Exploring various CIAM business and technical advantages
- Learning potential CIAM pitfalls

Chapter 2
Defining CIAM Value

Most companies have created custom solutions for Consumer Identity and Access Management (CIAM) needs because Identity and Access Management (IAM) solutions don't facilitate the business requirements I outline in Chapter 1. Additionally, Marketing often executes with external developer companies that have designed their customer experiences where registrations and authentication were initiated as a one-off. In a sense, you can call this shadow IT because this wasn't sufficiently supported by IT operations and can potentially create duplicate customer data sets. In addition, increasing legislation requirements are driving these practices to change.

Finding a Better Way

CIAM can be an on-premises solution or a Software-as-a-Service (SaaS) platform that handles marketing and product management needs to capture and interact with consumers. The functional requirements of a CIAM platform are optimized to facilitate registration, authentication, and profile management capabilities at scale. CIAM offers a centralized platform and data repository for identity profiles that links applications and services to individual user experiences.

At its core, CIAM consists of an external, consumer-facing interface designed to capture a combination of attributes that include name, email, mobile phone, address, and other personally identifiable information (PII) data. These fields are designed to effectively capture or register the consumer's data in relation to a campaign or content supported. In many cases of registration optimization, solutions like social login are introduced to speed up the authentication process by pulling social profile data into the CIAM identity profile. For example, when a consumer registers for a new account using a Facebook login option, the user is authorizing the use of basic Facebook profile data to establish a new account. Therefore, the user doesn't need to retype the same data fields for each new registration and can leverage a single social identity profile for new authentication requests.

REMEMBER

To avoid asking for more detailed or repetitive information at registration, CIAM solutions support *progressive profiling.* Progressive profiling entails requesting more PII as consumers advance through an experience or journey. Users only have to provide an address when a shipment is required or an age when alcohol or tobacco products are involved. As a result, consumers have an easier time registering with minimal data requirements, and their profiles grow the more they interact with the company. The objective is to design a frictionless experience to convert unknown users into customers.

As customers come back, they need to reauthenticate access with a username/password combination or even a biometric login to continue their personalized experiences. Behind the scenes, authentication mechanisms may include social profile integration, single sign-on, multifactor authentication (MFA), token-based approval, or a combination of these formats depending on the sensitivity of the use case. All users expect a smooth, easy-to-use login experience that's recognizable to the company brand image. Being consistent in the login and authentication experiences promotes trust and encourages usage, customer satisfaction, and loyalty.

Increased legislation drives consumer data and privacy rights. Consumers will need more control over their data at all times. Profile management on a CIAM platform is designed for providing a self-service capability for this purpose. Within profile management, the consumer's ability to edit, delete, and export data needs to be available. To understand the usage of this data, companies

need to define levels of consent that the consumer needs to approve prior to the data usage. For example, will the company be allowed to send promotional information, share data with third parties, or automatically analyze the data? The full business requirements of managing a customer life cycle are encompassed in a CIAM platform.

Understanding CIAM Advantages

CIAM provides many benefits. When you're evaluating CIAM platforms, each of the points in this section is important to consider when designing user experiences.

Frictionless experience with embedded security

CIAM systems provide services to the outside world where trust can't be assumed, so security safeguards to protect both data and account access are vital. Embedding high-level security technologies creates friction for the consumer in the registration process, which can lead to drop off. There's a delicate balance between the user experience and security.

REMEMBER

If you design a security threshold based on the risk profile of the use case, your consumers recognize risk in conjunction with the level of friction they're experiencing. For example, downloading a newsletter doesn't require the same level of authentication versus performing a financial transaction. When obtaining more identity information/identity proofing, make sure to establish trust levels to allow consumers to execute with minimized friction.

One method of protecting a consumer profile is to utilize MFA. MFA requires consumers to validate their identities by using a second method such as a mobile number or email. If the CIAM solution requires further credentialing, consumers can make a couple of assumptions:

- When users are informed of additional security details, the exchange of data results in higher security standards.
- Although sometimes cumbersome, having numerous secure login procedures provides assurance to customers that their data is safe when using applications or services.

A single customer identity

Unifying the customer view is required as consumers interact with your business through mobile, web, call center, and other emerging digital platforms. In the past, this meant trying to stitch together various data store information to hopefully create a centralized identity that could be leveraged for customer exchanges. Utilization of a CIAM platform allows the consumer to authenticate through a variety of channels, leveraging a singular identity. The end goal is for the backend systems of your company to only use one profile to validate the consumer identity. CIAM is basically a single point of truth for all consumer PII.

To understand the customer journey, collect different data points from external sources into an analytics environment. With one single consumer profile, the execution of analyzing this critical information has become much easier as a result of CIAM. Companies now have more accurate data to determine cross-sell, upsell, or personalized recommendations, which gives the consumer better experiences, increases satisfaction, and improves overall brand loyalty.

Managing clean data

The goal with CIAM is to establish a single source of truth by maintaining customer identities, attributes, and entities in support of reliable omnichannel customer engagement data. Managing clean data for your business applications can be expensive and costly if not properly maintained. With CIAM, a consolidated record of all data sources across numerous channels can improve data quality and support better customer personalization.

Consumers value personalized experiences that are relevant to them, so they'll keep their profiles up to date. For the company securing the application, it should leverage life cycle management tools as a way to keep data synced across various application stores. As a result, all backend systems use the latest information that the consumer provides.

Ability to market to one

Marketing organizations consider the ability to market to one as the end goal. It requires a lot of personalization to exactly target the wants and needs of a single person. A CIAM platform

becomes a single point of truth for consumer PII maintained by the consumer and connects directly into the marketing business applications.

When companies apply analytical capabilities on this personalized information in relation to their behavioral information, patterns can start to emerge. These patterns are used by the marketing applications to make suggestions to the marketer on how to deliver targeted content to the consumer. This way of personalized marketing has proven to be very effective to drive new revenue, which can be derived from the implementation of the CIAM platform.

Comply with privacy regulation

Businesses that store consumer data must adhere to federal, state, and local privacy compliance regulations. Applying compliance and regulatory controls is even more critical when a company has an omnichannel branded platform across multiple geographies. The European Union's (EU) General Data Protection Regulation (GDPR) is an example of a regulatory control that has a global impact if data flows in and out of the EU. The California legislature has implemented the California Consumer Privacy Act (CCPA) that follows the GDPR intent of protecting consumer data rights. Most countries either have similar regulations or are in the process of drafting similar alternatives.

REMEMBER

To ensure that your organization can maintain compliance with global regulations, CIAM allows for the following:

- Offers consumers full data access to their digital footprints across your platform and supporting systems
- Enables self-service privacy and consent for customer data
- Allows your consumer to determine what data should be discarded
- Provides to regulators auditable reports on data usage and consumer deletion requests
- Offers regulators documented processes on how you protect your customer data
- Demonstrates how you minimize data capture, in relation to the use cases, and avoids the free flow of data across your enterprise

CIAM is a highly customizable platform offering various configuration options to meet regional needs that are essential to any business operating worldwide.

Avoiding Potential CIAM Pitfalls

Engaging with consumers through digital channels means that trust needs to be established between both a consumer and a brand. Many of the pitfalls are based on the fact that engagements are designed from the viewpoint of the company.

WARNING

Inadequate planning for future consumer demands, constantly changing security measures, or even some mandatory compliance regulations can negatively impact an organization's ability to successfully execute.

Applying IAM to CIAM use cases

Enterprise systems that leverage legacy IAM are security centered. These systems lack the objectives of capturing consumer data effectively, supporting consumer workflows, and acknowledging customer demands. Even though IAM and CIAM use similar technologies, mixing data stores creates significant operational challenges around access for employees and consumers due to dual persona rights and privileges issues.

IAM assumes a level of trust as these solutions are deployed within corporate networks, but CIAM operates in an open and accessible environment. CIAM solutions are designed to operate using zero-trust principles. Every microservice has to authenticate to interact, and there's never a free flow of information without proper credentials.

Scale and availability

For companies, right-sizing an IT system is measured mostly by the number of users who are part of the organization. The number is measurable and somewhat finite. The user scale is contained often in the thousands and is priced accordingly. On the other hand, CIAM can reach hundreds of millions of users. The organization delivering a CIAM solution must create a platform that addresses performance and scalability despite varying degrees of user volumes. High-quality user experiences that eliminate wait

times must be delivered across all device types to avoid drop-off and abandonment.

Siloed data and access

Data must be actionable. Unfortunately, a majority of the customer-facing data that's collected by enterprise systems is siloed. Such data is often not available to other database management systems in the context of consumer profiles. Organizations that embark on implementing omnichannel marketing, sales, and service initiatives must agree on standardized attribute naming and access for their customer data. With CIAM, consumer data is managed centrally and made available to backend systems for effective use.

Systems integrations

WARNING

The biggest CIAM pitfall is to allow consumer information to flow freely across the organization. Because consumers now have ownership of their data, you need to be able to have control of this data at all times no matter where it's located. For example, Enterprise Resource Planning (ERP) systems, Customer Relationship Management (CRM) systems, or Learning Management Systems (LMS) must have different access conditions with granularity at the attribute level to assert qualified use of the data. The enterprise IT organization must be aware of the data utilization needs of Marketing, Sales, and Operations.

Organizations tend to use SaaS solutions or other third-party services to complement their business processes. Regardless of how the enterprise approaches the integration, the organization must evaluate the real needs of using the consumer data attributes. As you continue to be liable for the data you provided to these third parties, you must be able to execute on deletion/modification requests.

Security by design

Most applications today rely on Application Programmable Interfaces (APIs) as part of their technical framework. The CIAM implementation team must think about ensuring all development effort is utilizing secure touchpoints in the customer experience. What does this mean? The use of Security Assertion Markup Language (SAML), OpenID Connect (OIDC), and OAuth2, for example, could be used to handle a sizable data ingest. Any form of

sensitive data must be encrypted. It doesn't matter if the data is at rest, in motion, or in use, there should also be multiple forms of password protection, including hash- and risk-based protection.


REMEMBER

Organizations must consider numerous access control strategies as they design their CIAM implementations, including attribute-based access control (ABAC) and role-based access control (RBAC). ABAC is an authorization strategy that defines permissions using attributes whereas RBAC is based on assigned roles and responsibilities.


TIP

Even though all experiences are designed to use secure channels, measures like MFA need to be added to validate the consumer's identity and/or the device. With adaptive authentication techniques, you can reduce friction unless the interaction is suspicious or is triggered by abnormal behavior. Triggers can be created by using an unknown device, uncommon geolocation, or bot-like behavior.

Compliance and privacy

Strict guidelines are in place that vary from country to country on how to handle user data. Consumer-facing brands must comply with a country's regulatory policies if they're operating a public-facing information system that transmits personal data. The cost of managing these activities is extraordinarily expensive, both operationally and financially, to a company. Therefore, organizations must adequately budget for compliance and regulatory expenses.


REMEMBER

Companies need to ensure that consumers can execute on their data subject rights without any dependencies of the organization. This means providing full self-service for consumers, as the scale of CIAM makes it unmanageable to support them through call center interactions or other manual processes.

IN THIS CHAPTER

- Applying Enterprise Design Thinking
- Identifying essential use case requirements
- Explaining the CIAM framework
- Leading key stakeholders toward a CIAM strategy
- Understanding CIAM functional requirements

Chapter 3
Planning Your CIAM Strategy

Organizations of all types and sizes have their own unique use cases and security requirements. Regardless of customer type, all organizations can benefit from carefully planned Consumer Identity and Access Management (CIAM) deployments. A CIAM platform can remove numerous bottlenecks that traditional Identity and Access Management (IAM) solutions expose in the enterprise.

In this chapter, you discover business techniques that help your team think like a consumer. You find out what leadership roles are involved and what leaders want to achieve in the decision-making and selection process. Finally, you see how to develop a robust series of use cases that includes integrating functional requirements, which are essential to operational system success.

Enterprise Design Thinking

Enterprise Design Thinking is a framework that a business can use to collaborate, align teams, and form synergies when trying to solve a complex problem. Your business can apply modern

techniques, such as Agile delivery, throughout this process. This framework allows enterprises to explore user aspirations, needs, and pain points to drive better outcomes like a delightful user experience. Using Enterprise Design Thinking is especially useful when addressing the needs of both the consumer and business stakeholders when selecting a CIAM solution.

REMEMBER

Enterprise Design Thinking helps

- Design a more secure and effective user experience for your organization across various channels
- Create a common understanding among stakeholders and shared requirements for the user experience — developed directly by your users and stakeholders
- Secure future demand and widespread adoption of your CIAM solution across multiple lines of business

TIP

The most successful way to complete an Enterprise Design Thinking initiative is to conduct a workshop, bringing together all your business stakeholders: subject matter experts, line-of-business executives, and end-users. Let them explain their pain points and needs. Turn identified problems, wants, and risks into opportunities that become effective security solutions. Building a point solution shouldn't be the end goal; instead, plan a roadmap that includes insights and actions and assigns responsibilities to ensure the CIAM solution drives the best possible outcomes in your IT and business environments.

Gathering Use Case Requirements

Identification of your route to market for your products and services allows you to design your consumer experience and the places where you need to capture identity profiles. Because products and services are different across industries, enabling the right use cases is key to designing an effective CIAM solution.

When new business models are being developed, the process starts by defining the user storyboards and personas. The actual interaction between the persona and your product and services

is highlighted into journey maps and life cycles. Use cases are the result of these journey maps and life cycles, and are part of the product positioning and offering maps. As depicted in Figure 3-1, a new business evolves around the validation and understanding of a persona or identity. For this reason, a CIAM project program contributes significantly to the success and validation of the business model.

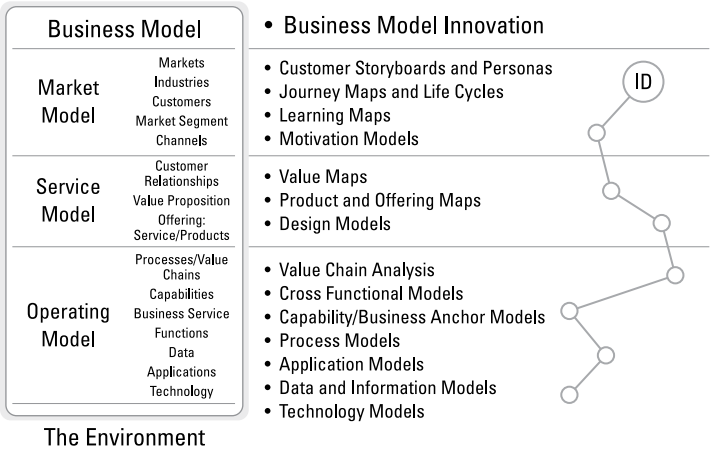

FIGURE 3-1: The model-based approach to gathering use case requirements.

WARNING

The market model approaches use case design from a "who is the user" point of view. Service models tend to be more product-centric. Operating models focus on tactical actions in day-to-day operations. Your organization should understand the size and scope of its target audience as well as technical needs. Most teams tend to use a combination of one or more methodologies in the design of a CIAM use case.

CIAM Framework

Many stakeholders are often involved in a CIAM conversation and as a result may have conflicting goals and objectives. Knowing your starting point with CIAM is an essential part of establishing

a well-defined CIAM strategy. A CIAM framework should include the following foundational building blocks:

- **Capture:** Capture is the collection of profile information in relation to the use case — for example, an email address to sign up for a newsletter. The capture effort is the company's way to entice unknown users to provide information with the benefit of an offer. This allows the brand to establish and start building a relationship with the consumer. As you build relationships with consumers, the user experience is just as important as the information you capture. To lower friction, capture also addresses the need to ask for information progressively as part of the user journey versus forcing a lengthy registration upfront.
- **Engage:** Engage is the level of security required to execute against a selected use case. For each use case, have a risk profile that justifies if additional security measures, beyond a password, are required. Additional measures could be multifactor authentication (MFA) or identity proofing as appropriate for engagement. Additionally, topics like multiple domains or data sources that require single sign-on should be addressed.
- **Manage:** Manage allows for full self-service of the data subject rights. Consumers should have access to all the content they've provided. As part of regulatory compliance, consumers should also be allowed to manage their consents in relation to the provided data and its usage. In principle, you're addressing this topic by allowing consumers secured access to their profile management environments.
- **Admin:** Administration is the operations and maintenance of an effective CIAM platform. The IT management team should focus on provisioning new web solutions or applications, reporting output creation, and integrating systems across the enterprise using a common data set. And this team should ensure appropriate policy and regulatory control enforcement.

TIP

Identify the right business stakeholders as you embark on an investment with a consumer identity platform. By focusing on the right framework, use case entry point, and an individual project owner, you'll have a higher probability of implementation success.

Addressing Stakeholder Needs

A successful program, for a new digital channel or service, requires collaboration between business and executive stakeholders to share their individual areas of expertise. Five types of stakeholders are vested in the CIAM life cycle. This section explains each stakeholder's role.

CMO

The chief marketing officer (CMO) focuses on customer experience, branding, and leading organizational marketing initiatives with an emphasis on an omnichannel experience for the user. The CMO aims to have a streamlined user interface (UI) regardless of the types or volume of consumer touchpoints. A marketing leader dictates that the interaction channels between the end-user and the brand experience are frictionless and drive conversion. CMOs are typically most concerned with the following:

- **Adoption:** Converting unknown leads to business opportunities and revenue is a critical part of the marketing role.
- **Single view of the customer:** No matter the customer interaction or information shared, a consumer identity profile needs to be captured and stored in a single centralized profile.
- **Analytics:** Marketing teams analyze customer trends, behaviors, and patterns to understand consumer motivation. Their goal is to build campaigns that support targeted promotion and personalization to create new revenue channels for the organization.

CIO

Organizations like to innovate, but they strive for standardization, reliability, and assurances when implementing new technology solutions. The chief information officer (CIO) makes decisions on the operational aspects of the platform and how to future-proof the organization's technical needs. Some of the key functional requirements when implementing a CIAM solution include

- **Reliability and scalability:** Companies can't justify any downtime, and consumers expect continuous availability. This expectation extends to high-volume events like holiday shopping and online sports events. Systems should scale quickly and efficiently to meet peak consumer demand.
- **Support for multiple use cases:** The CIO is looking for support for a variety of business demands that translate into various use cases. Having predefined configurations that support the majority of the consumer identity use cases is one of the selection criteria for a CIAM solution.
- **Resource skill requirements:** A full consumer experience is developed based on an array of skills ranging from web design and development, enterprise architecture, and IAM.

CISO

Security is a key consideration when implementing a CIAM program. The customer's profile contains sensitive but critical elements that define the relationship and success of the brand and its consumer trust. The chief information security officer (CISO) is responsible for protecting the security of the data assets. A CISO holds the responsibility over the following:

- **Password policy:** A strong password policy supports unique, generally non-repeatable use of passwords from a consumer.
- **Adaptive authentication:** The level of security required for the application should be based on policies that assess the degree of risk in relation to the use case. When the risk profile increases for consumers based on their profiles and behaviors, adaptive authentication dictates step-up measures such as security questions or MFA.

- **Secure, audited infrastructure and operations:** CIAM solutions can provide full-service capabilities. For example, with a SaaS-based solution, the CISO must protect a consumer's data from all touchpoints across the infrastructure by validating that the solution complies with regulatory controls and risk management criteria.

IAM team

The CIAM selection and stakeholder analysis process has been functional and C-level focused. The IAM team also plays a role — that of the developer and architect in the stakeholder analysis process. The IAM team is concerned with how to migrate and integrate across a multitude of applications and data sources. Furthermore, the IAM team primarily asks technical questions pertaining to security, authentication, authorization, device/profile management, polices/protocols, and delivery channels. The IAM team often breaks down requirements into authorization and authentication functionality, such as provisioning new projects, unlocking data for internal usage, and overall identity guidance.

CPO

Digital transformation has forced businesses to rethink the way the customer experience is delivered. The chief product officer (CPO) can't just deliver good products; he needs to address business and cultural norms in driving a winning strategy. Therefore, the role of the CPO isn't solely focused on tactical actions within product management. The CPO must focus on shaping products based on what users say, how they think, or what they do. Simply put, the CPO needs to resonate the voice of the customers, including how they may engage with one or more enterprise applications.

Addressing Functional Requirements

When you're conducting requirements gathering sessions, functional requirements are as important as the technical because if you don't understand the user's intent, then there is a high probability of system misuse. Technical requirements focus on

the protocols and implementation practices that stakeholders such as the IAM team would tackle. Functional requirements are those that the CMO, CIO, and CISO tend to concern themselves with when determining the best fit for a CIAM system. (Review the "Addressing Stakeholder Needs" section earlier in this chapter for more on role expertise and preferences.)

REMEMBER

Critical functional requirements to consider fall under four building blocks (see the earlier section "CIAM Framework" in this chapter for more info):

- **Capture**
  - **Traditional registration:** Email addresses, fraud check validations, existing account validations, password rules, and form requirements
  - **Social registration:** Access to viable social identity provider (IDP) sources, data available from social sources (gender, age, location), and account maturity/security risk potential
  - **UI:** Registration widgets (use pre-built Application Programmable Interfaces [APIs], code-based changes, workflow-only changes) versus developer created solutions (custom code to meet specific UI needs, usually a third-party engagement that needs to be aligned to stakeholder needs)
- **Engage**
  - **Login:** Type of user login (name/password, email/password, social/password, IDP alone, SSO), use of MFA, types of notifications (security, errors, workflows), centralized login capabilities
  - **Lockout and logout:** Single logout (time-bound or social), lockout policies (types, based on location, based on lists, validation rules), and step-up policies (risk-based authentication)
- **Manage**
  - **Self-management:** Execution of data subject rights, such as profile, consent, and password management
  - **Identity relations:** Account switching, parental governance, IoT relations, and federated access

» **Admin**

- **Provisioning:** Enabling admins, keys, apps, and users; creation of new users and applications; integrations with legacy systems and gateways; import types (profiles, passwords, attributes); profile management
- **Management controls:** Profiling (user, administrative); relationships (one-to-one, one-to-many, many-to-many), data exports (profiles, metadata to/from systems, log data), call center/customer-focused data (search and edit profiling), managing security controls, and breach monitoring

REMEMBER

Stakeholders must address several functional considerations outside of the technical requirements of implementing a CIAM solution. This list is a snapshot of how to best go about gathering requirements efficiently.

IN THIS CHAPTER

- Identifying CIAM feature guidelines
- Launching CIAM
- Following best practices for data migrations
- Seeing how successful CIAM operations run

Chapter 4
Recognizing the Deployment Requirements in CIAM

Planning and implementing a Consumer Identity and Access Management (CIAM) system requires both technical and functional preparation. Clear functional requirements drive the technical preparation for a CIAM solution selection. In this chapter, you find out how to select a CIAM solution based on these requirements and become familiar with the data migration and integration processes. Finally, an introduction to two common CIAM use cases helps you understand the solution potential.

CIAM Feature Guidelines

When organizations decide to select CIAM as an identity management platform, as part of the requirements and deployment process, they should consider these four guidelines:

- **Frictionless user experiences:** The platform should support the same consumer experience for any communications channel across domains. Consumers require a secure

experience to complete any identity-based function for login, registration, or workflow.

- **Rapid development and integration:** CIAM solutions rely on connectors, Application Programmable Interfaces (APIs), or development tools to rapidly integrate data and application sources between legacy systems and the CIAM platform.
- **Centralized access management:** Centralized consumer profiles, access policies, and privileges are essential in streamlining an efficient and cost-effective CIAM program. The consumer's data is self-managed and up-to-date, so it can be utilized by various business applications to provide consumer services without requesting the same information or accessing credentials over and over again.
- **Compliance and regulatory policy:** The platform must support the requirements for data subject rights and access controls and meet compliance standards with industry and government/country specific regulatory restrictions that impact customer-facing interactions. A secure CIAM solution is critical to winning consumer trust.

REMEMBER

Mature CIAM platforms offer a seamless end-to-end customer experience, integrating best-in-breed security features while also drawing on analytics capabilities to help strengthen the customer experience channel.

Taking Steps to Launch CIAM

In the CIAM marketplace, solutions are generally delivered via Software-as-a-Service (SaaS). The SaaS solution may be multi-tenant but can also deliver a client-segmented data store, while providing the platform framework. Organizations that decide to embark on implementing CIAM must determine which deployment option is best suited for their needs.

TIP

Technical decisions, including upfront licensing costs, shouldn't be made solely on price; however, as your organization scales, price may become a significant factor in sustaining your solution. You must consider development, maintenance, and downtime. Plan for growth and long-term viability. Consider the following when planning:

- **SaaS:** Usually, pricing is per user or profile inclusive of infrastructure and associated risk management of the environment.
- **Managed service:** Pricing can be based on instance or identity inclusive of labor services for management of the environment and software configurations, updates, reporting, and troubleshooting.
- **On-premises or private cloud:** Pricing can be calculated per user, server, or transaction, exclusive of hardware, environment security, regulatory compliance (for example, PCI-DSS, HIPAA, ISO27001, or NIST800-53) and management services. Scalability, particularly the capability to grow dynamically with customer needs, should also be addressed during the selection process.

Decide if your organization wants to approach CIAM as being the only hosted instance of the application handling your array of data sources and applications (single-tenant). Alternatively, would there be any hurdles if there are many hosted clients on the same server instances that can handle your data and applications (multi-tenant)?

TIP

Consider a single-tenant approach when

- An application is associated with a single customer.
- Customer branding is associated with the login or across the omnichannel experience.
- Connection-specific access to the customer should be available to end-users.

Business-to-Business (B2B) and Business-to-Customer (B2C) organizations are apt to approach CIAM using a multi-tenant, SaaS-based approach. However, each of those customers has its own domain. Each user is running its instance of the application. Even if many applications and data sources will aggregate into the multi-tenant application, the domain itself is exclusive as it has its own set of requirements within the tenant.

TIP

Consider a multi-tenant approach when

- A single login page exists for many applications.
- All users across all application tenants will exist in a single database for the domain.

- The organization doesn't require per-customer branding on each login page.
- End-users may belong to more than one domain, so they may need to log in to more than one tenant anyway.

REMEMBER

Most organizations prefer SaaS by default, which is multi-tenant because of cost, scalability, and reduced burden to the organization in managing policies and protocols.

Undergoing Data Migrations

After you select your CIAM vendor, data migration is a task that you must undertake, and it can be one of the most challenging aspects to a CIAM program. Most organizations must acquire data from more than one enterprise system. Across the CIAM marketplace, you'll find that vendors have connectors or pre-built APIs, making it easier to support data ingestion from legacy systems to a CIAM system. However, these integrations aren't always sufficient. All systems should include — at a minimum — one of four data migration options:

- **Standard migration:** Taking records from legacy systems and importing them into a cloud identity store using the standard import/export protocol
- **Custom data migration:** Requires a two or more-step process to de-duplicate and transform data that doesn't conform to the CIAM system, often resulting in a transformation challenge related to encryption or data type mismatches
- **Data mapping and transformation:** Requires data transformation and likely conversion from an unstructured format to a more structured format in the CIAM system of record; must conform to a standard naming convention to support credential mapping
- **Connectors and API-based migration:** Referred to as self-managed migration

  Most platforms have developed a series of connectors to ingest data between hundreds of legacy sources, social, and enterprise applications into the centralized CIAM data store. The bi-directional synchronization, once configured, is hands-off to the administrator and end-user.

Data migration is usually a one-time event per data source instance. After completion, the application synchronizes the ingested new data between the legacy system and the CIAM solution. If appropriately configured, the data migration process offers flexibility, scale, and optimal performance while creating minimal disruption to the customer experience.

Managing Data Integrations

Choosing CIAM is preferred by organizations because of the capability to integrate with resources across the enterprise. The solution offers the following features:

- Connects to legacy applications via authentication adapters
- Records document repositories (structured or unstructured) that can connect using an authentication adapter
- Reduces infrastructure management by using cloud-based Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) offerings
- Increases business productivity with SaaS applications
- Uses big data analytical tools to analyze data and metrics
- Contributes to e-commerce/m-commerce
- Manages Internet of Things (IoT) devices and sensors
- Gains more efficiency through mobile applications

After application integration and enablement occur in the CIAM central administrator, users can self-manage their identities across one or more apps consistently. CIAM, by default, creates self-sufficient consumer empowerment. Figure 4-1 shows how numerous data sources and apps can seamlessly integrate into a multi-tenant SaaS CIAM environment.

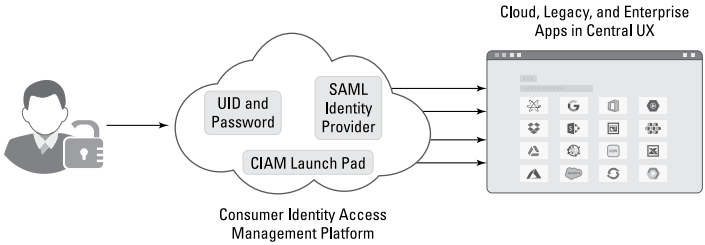

FIGURE 4-1: An example of CIAM data integration.

REMEMBER

It's not uncommon for application integration to be a mix of legacy and cloud-based systems, hence a hybrid deployment. Seldom will a CIAM deployment be 100 percent SaaS-based with regard to data integration. Many organizations still have an on-premises or a data center footprint with applications requiring support. The challenge remains the same across environments: accurately mapping the data sources across the enterprise.

Running Successful CIAM Operations

Organizations choose to use CIAM for several reasons: customer centricity, central administration, ability to scale operationally, and analytics. In this section, you discover two use cases in which CIAM has excellent potential as an identity management platform for consumers.

Customer service applications and CIAM

Data is the most precious commodity to any marketing team. Associating an account with a name is no longer enough. To implement an aggregate view of all data and truly leverage the consumer profile in omnichannel campaigns, CIAM has strong potential.

TIP

CIAM systems offer customer service applications the following benefits:

- Provides a secure, seamless single point of entry customer experience for end-users
- Allows the company to acquire and recognize customers through matching
- Supports accurate data mapping options
- Facilitates contextualized marketing options through systems integrations by using connectors or authentication protocols

Customer service applications, such as email marketing systems, CRM, or e-commerce platforms, require an IAM solution to register, authenticate, and manage the identity of a customer to one

or more applications. Systems integrations across each of these applications should be seamless.

What CIAM offers to the marketing team is access to rich user engagement data. Leveraging the aggregate data collection found in a centralized data store potentially creates a compelling knowledge profile on users. Marketing can drive actionable campaigns across channels with these rich insights.

For marketers, the use of a CIAM platform is a win-win. The rich data collection from CIAM can be tied to consumer service applications to support the creation of an end-to-end customer journey with an emphasis on behavioral intent and corporate profitability. The platform also has the potential to transform sales, marketing, and operations teams due to the analytics it provides for the enterprise.

IoT applications and CIAM

The IoT is a network of connected devices that collect and exchange data. The use of IAM tools in IoT is expanding rapidly because devices often interact with people, access points, and data types. There is general consensus that access to IoT-enabled technology can pose a significant access risk. Instead of focusing on access, attention should be on protection and defense measures.

WARNING

Most IoT devices or systems come with default passwords. Users should change these passwords immediately. Lack of compliance poses a challenge with managing credentials. Even when users change their passwords, users can pick passwords that are easy to hack.

Stronger methodologies must be put in place on IoT devices to protect passwords, including encryption alternatives. Encrypting a password provides a level of uniqueness so an unlawful party can't intercept the data maliciously.

There are some risks with mandatory password management and encryption. Sometimes users will gain access to the system unnecessarily or be restricted unintentionally.

TIP

Some recommendations for implementing one or more IoT solutions with CIAM include

- Establishing an IoT device registration process
- Understanding how regulatory and compliance policies impact all your data interaction points
- Designing flexible authentication and authorization policies for connected devices
- Using end-to-end encryption to protect data endpoints
- Applying preference and consent management to all IoT user-based systems
- Supporting contextual control using adaptive authentication and data access regulations throughout the enterprise

IoT offers yet another opportunity to connect consumers with brands. The role of CIAM in IoT architecture must consider data protection strategies. Otherwise, consumer and enterprise data are mutually vulnerable to unwanted threat actors.

IN THIS CHAPTER

- Succeeding with CIAM
- Identifying CIAM features
- Selecting and deploying a CIAM system
- Investigating cloud vendors

Chapter 5
Ten CIAM Planning Items

Addressing the needs of the consumer can be a challenge when selecting, implementing, and deploying a Consumer Identity and Access Management (CIAM) solution. While authentication and authorization are crucial to securing a central repository, organizations should also consider many non-technical features during the evaluation process. Support documentation won't provide these experiences that come from being in the field. The suggestions and warnings in this chapter are best practices across leading industry vendors.

Identify Your Target Audience

Consumers demand user experiences that meet their needs. If users' needs aren't attainable, they won't interact with a platform. Abandonment can occur even before users log in and authenticate without ever providing the organization an idea of who they may be. You need for end-users to log in to the website so every interaction is trackable. Frequent customer interaction helps build a unique profile and method to create a targeted audience experience.

Both consumers and marketers seek control and privacy across all interaction points. With CIAM, marketers gain valuable insights across comprehensive data sets once aggregated into a centralized

database. The customer gains convenient access using a singular entry point regardless of platform using CIAM to review all their data. Marketers gain the analytics and insights needed for personalized offers; the consumers get a more frictionless and contextualized user experience.

Design for an Omnichannel Experience

Enterprise applications aren't consumer applications in that consumers aren't forgiving. Users expect that no matter what device they interact with, their interactions with the platform will be consistent. When it comes to login access, users abandon platforms if they don't understand how to access the login pages efficiently or if the online system takes too long to grant access. Chapter 2 covers this idea in more detail.


TIP

A consumer-facing system must provide a lightweight, self-explanatory user experience. The system should provide timely, informative feedback to the end-user when performance isn't optimal. Interfaces shouldn't be complicated or vary between channels. These techniques ensure reliability, satisfaction, and return intent.

Plan for Repeatable Use Cases

The lines often blur between IAM and CIAM use cases. While the IAM use case is employee-centric, and the CIAM use case is consumer-facing, an overlap in features across both use cases is more commonplace. Password and user management, account provisioning, and single sign-on are common in the enterprise and with the consumer. Across industry verticals, the requirements can vary from a technical perspective. The differentiator is the presentation layer across the applications.

In creating an omnichannel platform, organizations must plan for adaptive access or continuous authentication. Standard authentication techniques such as usernames and passwords negate context-sensitive psychographic data collections. Yet, adaptive access offers the best of both worlds to the customer and marketing team.

REMEMBER

Enterprise projects aren't one-off exercises. They're a way to create significant results for an organization's productivity and financial viability. Check out Chapter 4 for examples.

Prioritize Deployment Strategy Use Cases

Often organizational demands for the use of social identity providers (IDPs), big data applications, and attractive user platforms aren't adequately accommodated by traditional IAM solutions. The scale and complexity of user data, the contextual parameters that drive engagement, varying integration needs from the business systems, and ever-changing compliance requirements of government agencies globally all play a role in the deployment strategy (I cover deployment strategies in Chapter 4).

TIP

Find applications that have similar identity structures that can hasten repeatable deployment opportunities. This path is your quickest way to market and may include looking for applications where the IDP requirements are reasonably consistent with regard to username and password. Additionally, evaluate applications where user demand is the most significant and the migration time from the legacy environment to CIAM will have a minimal impact on user productivity.

WARNING

Make sure any time there's a new deployment, such as a new feature set, that it adheres to the consistency and richness of the user experience. Any performance degradation may negatively impact consumer satisfaction and future usage.

Establish Consumer Self-Service and Profile Management

To support global CIAM across any number of sources, organizations aggregate data to establish a frictionless single sign-on experience (see Chapter 2 for more info). Data sources may include social IDPs, mobile applications, web applications, enterprise IDPs, and front-end user interfaces (UIs). These source integrations help enforce a single user profile that may otherwise have been accessible independently, creating a fractured interface for user engagement.

Many financial benefits exist for those who use CIAM to support self-service and profile management. Having a single login reduces the number of usernames and passwords that a customer must remember. With fewer accounts to manage, there's often a reduction in help desk costs. The added benefit is that the users become empowered to manage their own accounts. Users are far less confused in credential management, thereby increasing self-service account recovery. Even when multifactor authentication (MFA) is in use for an application, one set of required credentials can reduce user confusion when having to log in to many apps.

When many application integrations exist, the data collection opportunity is tremendous. More data provides a contextually focused end-user experience in an attempt to simplify interactions leading to self-service management.

Design Operations for Continuous Business Support

CIAM presents both consumers and the enterprise with a golden opportunity. Vendors offering modern web-based, mobile, or Application Programmable Interface (API)-centric applications have few integration issues with CIAM solutions. The solutions from these vendors are usually commercially available, which means they tend to work with many IDPs. Why? Such platforms are data-rich, offering new potential streams of income and partnership synergies. Those applications that are homegrown, highly configurable, or legacy-based with complex security architectures tend to present the most significant risk to systems integration, potentially impacting business continuity.

Being laissez-faire isn't an excuse when supporting a customer. If a customer's data is compromised, the onus must fall on the organization to take swift action. Upgrading the legacy application to a more modern standard, decommissioning a system if it lacks a meaningful purpose to a customer, or consolidation of systems into a centralized solution are examples of being proactive to ensure business continuity.

TIP

Many Software-as-a-Service (SaaS) vendors create connectors and API packages that enable active support and integration with their CIAM platform. Leveraging a commercial CIAM solution should maximize out-of-the-box connectivity, support ease of data migration, and promote minimal system disruption at all times. These three benchmarks are the hallmarks of designing for continual business operations.

Evaluate Operational Maturity and Capabilities

Every IT vendor provides a list of best-in-breed features to customers as part of the selection process. It would help if you asked yourself specific questions. Outside of the CIAM solution, what other product synergies does a vendor offer? Does the vendor have a complete ecosystem of threat management and digital identity protection products? What level of research and development investment are these vendors putting into their CIAM offerings? Do they collaborate with industry peers to strengthen the security marketplace? Are they also leaders in other cloud compute product categories?

If the answer is yes to most of these questions, you have found a mature, capable vendor. An operationally mature vendor engages with its peers, makes constant research and development (R&D) investments, builds other leading security products in the market, and also is a leader in the cloud market. Products that offer many systems integration options with industry partners are also likely operationally mature.

Monitor and Support Continuous Improvement and Security Risk

IAM solutions are part of a broad IT toolkit for continuously monitoring security conditions, maintaining awareness of information risks, and protecting organizations from vulnerabilities and threats. IT vendors are always trying to enhance their IAM products as the security landscape rapidly changes. Enterprise IAM is often internally facing, but CIAM is consumer-facing, which comes with far more compliance and regulatory oversight from government agencies.

REMEMBER

Systems must not only protect a user's private data but also meet the auditing and regulatory reporting requirements for those countries where an organization conducts business. Organizations should be concerned with auditing processes and data regulations such as the General Data Protection Regulation (GDPR), Healthcare Insurance Portability and Accountability Act (HIPAA), Children's Online Privacy Protection Act (COPPA), and Payment Card Industry Data Security Standard (PCI DSS), and the actual monitoring of their personal and server compute environments.

Infrastructure is a first-line target for hackers. These systems require the most protection, which includes lock-down or limited access to a subset of users. If a system maintains any form of user information, including credentials, auditing and monitoring should occur regularly. Methods to monitor information risk may include manual or automated techniques such as network scanning, penetration testing, API and code set evaluations, and regulatory best practice review.

Create Actionable Metrics

Analytics output coming from the data ingested in a CIAM system provides unique opportunities for customers and company leaders. One benefit of CIAM is that you can create actionable metrics for dashboards, reports, and audits. The development of fine-grained actionable reports on how users interact with the system allows IT to evaluate security concerns and Marketing to observe consumer behavioral intent. The sum of such outputs can also support regulatory and compliance reviews to meet country-specific regulations. You can then run regular standard reports on specific users, domains, or application-based activities to ensure operational and business continuity within the confines of governance and policy controls.

Actionable analytics and the outputs are not only a function of the IT team but also help marketing operations. Demographic and psychographic data measures help the enterprise better understand how to target customer activity. Targeting customer activity translates into profit. Developing reporting solutions that offer deep insights, given the plethora of big data analytics and alert controls available, provides enormous potential to Marketing in creating niche, contextually reliable marketing solutions using behavioral-based actions and user credentials.

IBM Security

IBM Security Consumer IAM Services

Enable on-demand, personalized, and trusted experiences between consumers and brands

– Adoption strategy and design
– Accelerated CIAM deployment
– CIAM services on-demand

IBM

Discover CIAM services

In this book, you find out about the business drivers, technology, and capabilities of Consumer Identity and Access Management (CIAM) solutions. Discover practical advice and strategies to plan and deploy a successful CIAM platform, while avoiding potential pitfalls.

Inside...

- How CIAM differs from workforce IAM
- Various deployment models
- Potential CIAM pitfalls
- Key CIAM use cases
- Strategy considerations
- CIAM functional requirements
- Compliance and regulatory benefits

Martijn Loderus leads IBM Security's global CIAM services practice.

ISBN: 978-1-119-71560-3
Part #: W0WNKGNP
Not For Resale

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.