IBM Security

Bringing stakeholders together to modernize CIAM across the organization

IBM

Get started

Introduction

When you register a new account, make a purchase or even sign up for a newsletter, you are trusting an organization with your personal information. After that initial exchange, you likely don't want your information used for purposes outside of what you agreed to, but with your consent perhaps you would appreciate personalized experiences and recommendations for the future. The important thing is this is up to you, and you can change your mind at any time. And if you experience any friction throughout your interactions or start to lose trust in the organization for any reason, you'll likely abandon it and find another. Consumer identity and access management (CIAM) enables these on-demand, personalized and trusted experiences between consumers and brand, and as a consumer yourself, you can empathize with your own consumers as you consider updates to your organization's digital strategies to stay competitive.

CIAM, however, is much more than a website update or a marketing project; it impacts functional areas across the organization as touchpoints with consumers are evaluated and modernized. To ensure the timeless balance between convenience and security doesn't tip, organizations must bring together both business and technical stakeholders to acknowledge CIAM as an outcomes-focused subset of digital transformation that can share technology components with workforce IAM. When implemented strategically and purposefully, organizations can maximize their engagement with consumers while minimizing risks for IT and security personnel.

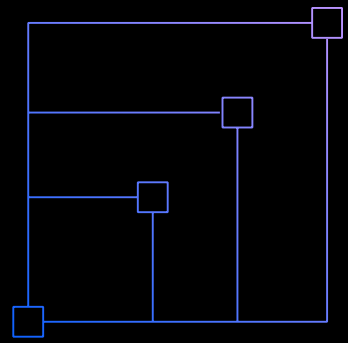
Without a CIAM strategy, businesses risk losing revenue due to customer abandonment; brand loyalty remains fragile when alternatives lay at their fingertips. Similarly, in the public sector, government agencies still primarily holding onto legacy infrastructure and processes may lose the confidence of their citizens and fail to obtain ideal levels of public service adoption. Despite differences in their missions, both the private and public sector relate in their need to serve consumers with a frictionless yet secure digital experience to facilitate privacy-aware information sharing. And many organizations have taken note to do just that, causing CIAM to become the largest segment of the total IAM market, forecasted to grow 15.1%[1] annually through 2025. For those that have not yet started their digital modernization, one of the first and most important steps is creating leadership alignment across several functional roles so that all can benefit from the project.

Chief Marketing Officers (CMO)

CIAM Goal: Capture, nurture and grow users through personalized experiences that are privacy aware and user controlled.

Across the private sector, marketers are fighting for the attention of potential customers, and the last thing marketers want is for a difficult registration experience to drive customers away at the last minute. Customer abandonment can have a direct impact on revenue, thus CIAM programs aim to streamline registration and onboarding experiences to avoid this problem and convert unknown leads into business opportunities. Ideal onboarding forms will request as little customer information as possible, with touchpoints appropriately set up to progressively learn more about a customer as the relationship grows.

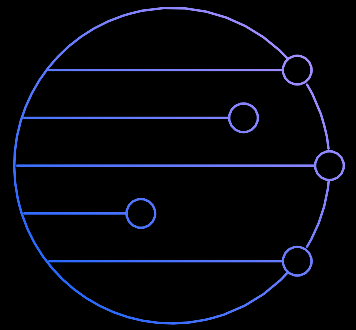
Large organizations with multiple sub-brands should architect their data stores to maintain a single identity for each consumer, integrating with customer relationship management (CRM) and other third-party tools and systems along the way. With consumer identities centralized, strategic implementation of CIAM best practices will enable marketers to better understand their consumers' behavior and run more targeted, personalized marketing campaigns. CIAM plays a central role in the digital experience for both prospects and customers, so it is natural for marketing leaders to play a key role in the modernization planning process.



Line-of-Business Managers

CIAM Goal: Deliver a streamlined, frictionless experience with modern interfaces and engagement to help meet goals of the organization

Business managers or agency owners are similarly driven to onboard consumers and enable smooth interactions, although not necessarily for revenue's sake. For instance, government agencies must efficiently provide public services to citizens and modernize engagement across a vast span of user preferences and channels, typically without a true marketing function in the organization. Agency owners seek similar transformation of the user journey to simplify registration and reduce abandonment to ensure successful delivery of services. While they may not be running any marketing campaigns, these business managers still aim to achieve a single identity for each consumer to streamline consumers' interactions across departments, eliminate redundancies and better understand behavior.

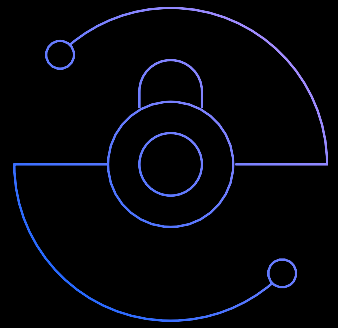


Security and Privacy Officers

CIAM Goal; Deliver secure consumer interactions to prevent user fraud and account compromise, provide transparent and user-controlled experiences and maintain compliance

As a guiding principle, consumers should know who is in control of their data and how it is being used, with the opportunity to self-service their own data and modify their consent at any time. This is enough of a reason for organizations to prioritize privacy and consent management for their digital experiences, but global regulations insert some forced urgency to the issue. Enterprises must follow each region's rules in which they operate or risk hefty penalties and fines, and while the privacy laws go into detail regarding what organizations are required to do, they don't typically provide specific instructions for how to get there. A proper CIAM implementation acts as a single source of truth for all personally identifiable information (PII). Privacy officers and compliance experts can define rules and policies across various consent management purposes that technical staff simply apply across necessary apps. This allows privacy and compliance personnel to move beyond spreadsheets and meet the dynamic reality of privacy laws and make them more approachable.

While CISOs will share interest in privacy and consent management along with privacy and compliance officers, it can sometimes be tempting for CISOs to think of CIAM overall as a marketing project and lose interest compared to other priority initiatives. The outcomes of traditional workforce IAM and consumer IAM are indeed quite different, yet both will benefit from commercial solutions that store data securely and help mitigate the risk of data breaches—both employee and consumer identities are worth protecting. In addition, if CIAM initiatives proceed without strategically considering the current state of IAM infrastructure, the CISO may end up with additional piecemeal solution fragments in their organization's environment, increasing risk with additional points of access. It is in the CISO's best interest to bring workforce and consumer IAM use cases together under a single solution when possible to prevent unnecessary data siloes.

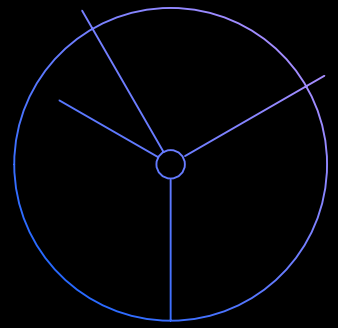


Chief Information Officers (CIO)

CIAM Goal: Reduce complexities of adopting and maintaining IAM solutions while keeping up with the latest identity standards to maintain a modern security posture

Consumer engagement benefits of CIAM aside, the CIO must evaluate each new technology decision for fit within the organization's holistic infrastructure and operational plan. Simplicity and standardization are ideal, so marrying IAM and CIAM functionality in a single tool should resonate with IT leadership just as it does with security. With this approach, the overall IT environment does not grow in complexity, nor does it require any new skills from existing staff. There will likely be a cost benefit to reusing the same solution for external populations as well, keeping overall IT operating expenses to a minimum.

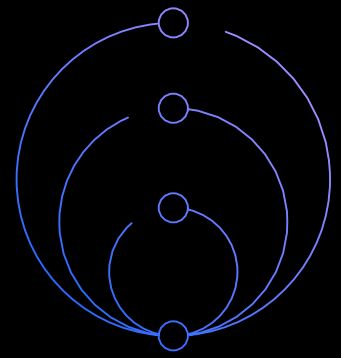
Once a CIAM solution is up and running, every minute of downtime can mean detrimental lost time and revenue to those organizations whose customers can't access their accounts. This alone would explain why many IT leaders prefer cloud-based solutions for CIAM use cases from a return-on-investment perspective, as they tend to offer much higher availability and scalability than on-premises alternatives. Still, cloud IAM offers additional incentives for IT staff like reduced infrastructure maintenance, automatic software updates and faster time to value.



IAM Admins and Developers

CIAM Goal: Simplify development work and protect and maintain application policies through low-code and configuration-based workflows

While executive stakeholders align on higher level business objectives, operating costs and risk mitigation, IAM admins and developers can influence the CIAM program development by evaluating solutions' technical capabilities across the board. They can look at logistics for migrating or merging data sources and applications, plus key items like supported authentication protocols, MFA methods and delivery channels. To achieve quicker time to value, this team can evaluate solutions' API documentation, guided resources and low-code experiences as well to ensure their team will be well supported through solution implementation and maintenance. Workflow-based capabilities like consent management in the CIAM tool may save developers headaches for instance by abstracting detail from privacy laws to simple API calls that automatically account for changing requirements. Before yet another tool is added to the mix, technical personnel should holistically assess compatibility and integration with their existing IAM solutions to ensure an optimal fit for the long term.



IBM’s Integrated CIAM Approach

Modernize Digital Experiences with IBM’s Integrated CIAM Approach

With IBM Security, your organization can capture and connect with your consumers through on-demand, personalized and secured omnichannel engagements using a blend of identity strategy, digital design expertise and cloud native CIAM technology. By using IBM Security Verify coupled with IBM Security Services, you can help build organizational alignment, track consumer information respectfully and accurately and delight consumers with simple, secured digital experiences of your brand.

Next steps

Go deeper with CIAM
Read more about CIAM best practices, planning considerations and pitfalls to avoid

Download the guide →

Explore IBM Security Verify
Use IDaaS to modernize user experiences through social login and adaptive authentication while preserving privacy with consent management

Learn about Verify →

IBM Security CIAM Services
Plan, design, deploy and execute a CIAM program against business goals using a unique consultative and collaborative approach

Get help with CIAM →

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
February 2021

[1] Markets and Markets, Consumer IAM Market Global Forecast to 2025