CIAM Buyer’s Guide for Financial Services

Choose the Right CIAM Provider
for Your Needs

GUIDE

Table of Contents

The Imperative for CIAM Modernization

The financial services industry is changing at an unprecedented pace. Amidst an evolving regulatory landscape, new technology, market forces, and growing consumer demands – one thing is certain – keeping ahead of fierce competition is about maximizing returns on digital investments.

The emergence of financial technologies (fintech), digital-first banking, and cloud-native providers presents industry incumbents with competitive risks and opportunities to develop seamless, secure, and scalable end-to-end customer experiences.

Meanwhile, the growing cybersecurity threats posed by crime syndicates, persistent threat groups, and rogue state actors continue to compound the risk of fraud, account takeover (ATO), unauthorized access, and regulatory breaches.

These challenges are further amplified by changing customer engagement patterns, privacy regulations in many parts of the world, and the rapid growth of the third-party financial services ecosystem within and across global regulatory jurisdictions.

Beyond that, financial services organizations are increasingly looking to capitalize on increasing their adoption of open banking, open finance, banking-as-a-service (BaaS), and embedded finance to accelerate hyper-personalization, extend reach to new markets, and create new value-added revenue streams in what is a highly competitive industry.

CIAM as a Strategic Asset

The capacity to achieve these goals is more than ever shaped by their ability to detect, respond to, and prevent fraud, mitigate cybersecurity risks, and achieve regulatory compliance, while delivering seamless, secure, and scalable customer experiences. It's, therefore, no surprise that financial services organizations can no longer rely on outdated customer identity and access management (CIAM) legacy, or a myriad of fragmented point solutions that impede digital agility, fail to meet complex use case requirements, and further deepen exposure to fraud and cybersecurity breach. This is precisely why CIAM has become a strategic asset across the industry.

Deciding to embark on a journey of CIAM modernization, helps financial service organizations unlock novel ways of combating fraud across the end-to-end customer journey, accelerating hyper-personalization across web, mobile, and hybrid channels, securely expanding reach across the third-party ecosystem, and reducing costs, impediments to digital transformation, while gaining access to cutting-edge CIAM innovation – all in one platform, available in self-managed, hybrid, and SaaS settings.

This guide is designed to help your organization navigate the complexities of selecting a new CIAM vendor and embarking on your modernization journey. By understanding the critical elements of CIAM, your team can make informed decisions that align with their strategic objectives and digital transformation goals.

The way forward is clear: to stay competitive and secure, financial service organizations must adopt a CIAM approach that is flexible, scalable, and capable of delivering personalized experiences. CIAM not only helps in safeguarding against threats but also plays a crucial role in building and maintaining customer trust and loyalty.

DID YOU KNOW?

52% of consumers will go out of their way to buy from their favorite brand.
– Semrush

Embarking on Your CIAM Journey

Starting your CIAM journey requires a strategic approach. Are you looking to strengthen fraud detection at the account onboarding and identity proofing stage? Are you looking to enable secure integration with third-party providers (TPPs) via financial-grade APIs? Are you looking to build a real-time view of needs across all channels to accelerate upsell? Or maybe it’s all of the above!

Once your objectives are clear, the next step is to choose the right CIAM approach. This involves evaluating your current identity infrastructure and identifying opportunities for CIAM modernization. It’s crucial to consider both functional and non-functional factors such as security features and the ability to deliver personalized experiences, along with scalability and deployment options.

A successful CIAM strategy is primarily about aligning your identity management practices with your broader business goals–and then finding the technology that can deliver. Whether you are enhancing customer loyalty to drive retention and revenue growth, or ensuring compliance with regulatory requirements, your CIAM solution should be a key enabler of these objectives.

By adopting a strategic approach to CIAM, your organization can ensure that it is well-positioned to meet the evolving demands of its customers and maintain a strong security posture while future-proofing investments for years to come.

> “By 2026, 25% of IAM leaders will be responsible for both cybersecurity and business results, operating from the C-suite as CIDOs.
>
> – Gartner, Predicts 2024: The Changing Role of the Identity and Access Management Leader, Michael Kelley, Rebecca Archambault, Nathan Harris, Henrique Teixeira, Oscar Isaka, 1 December, 2023

Getting Started with the Basics

The first step in the process is to start with some high-level questions to streamline the list of vendors to which you'll apply the more elaborate evaluation criteria in the next section. Evaluate these higher-level questions to get started.

Question	Why it matters
How long has the vendor been in business?	Experience in the market can indicate stability and a track record of success.
Is the vendor a recognized leader within the industry?	Third-party recognition of leadership often reflects innovation, reliability, and a strong customer base.
Has the vendor demonstrated expertise in solving complex identity problems without large, post-sale surprise costs?	While most vendors can solve basic use cases, their costs compound exponentially for customizations that are required by most large projects
Can the vendor provide customer success stories and testimonials that relate to the problems you're trying to solve?	Real-world success stories provide insights into how the solution has performed for other organizations.
Has the vendor applied sufficient rigor in securing customer deployments?	A strong security posture is a critical requirement for ensuring customer data and mission-critical infrastructure are insulated from attack.
Has the vendor delivered performance and resiliency at a sufficient scale?	Delivering at scale is critical to being competitive and being able to expand within both internal and third-party ecosystems.
Does the solution allow you to easily design A/B tests to optimize the customer journey?	A/B testing is critical for improving conversion rates and retention by optimizing customer experiences.
Does the vendor have a track record of innovation to meet evolving industry and customer demands?	Continuous improvement ensures that the solution stays ahead of industry trends and evolving requirements.
Does the vendor offer robust training, support and an active user community?	Strong support and training resources are essential for successful implementation and ongoing use of the solution.
Does the vendor have a strong implementation partner network?	Skilled IAM practitioners can be hard to find. Having skilled partners ready and able to make your implementation successful is critical.

Of course, you also need to evaluate vendors' capabilities to meet your specific objectives and requirements. To help you do that, we've provided an overview of CIAM capabilities, evaluation criteria, and details about why each is important.

The criteria are organized such that they continue the alignment between common business initiatives and customer identity capabilities, while adding other important criteria considerations, such as compliance, implementation, and operations. In establishing your evaluation criteria through this lens, you'll be able to prioritize the capabilities that will make the greatest impact on your organization's specific objectives.

> We're not just looking at identity as a one-off, but rather the identity lifecycle. We need things like policies and consent services, but those should be both seamless and easily explainable to the customer in order to deliver a great experience— that is very important to us. So, it's about the features as well as the usage, and that's why we have chosen Ping Identity.
>
> – Deniz Güven,
> CEO, Mox Bank

Evaluation Deep Dive: The Comprehensive Criteria

Let's dive into the specific capabilities you should evaluate when choosing a CIAM vendor. We've divided this section into subsections based on the category groupings as follows:

1. **Acquisition, Onboarding, and Verification**
2. **Fraud Prevention and Security**
3. **Customer Experience**
4. **Regulatory Compliance**
5. **Revenue and Loyalty**
6. **Implementation and Operational Considerations**

Acquisition, Onboarding, and Verification

The criteria in this section focus on converting your prospects into new customers, taking them through identity proofing, account onboarding, and enabling them to seamlessly start interacting with your services.

Capability	Evaluation Criteria	Why It Matters
Orchestration	Does the solution allow registration, authentication, and authorization journeys to be easily created, viewed, and changed with no-code/low-code drag-and-drop user interfaces?	To provide secure, effortless customer journeys, a CIAM solution should provide organizations with no-code/low-code identity orchestration capabilities. With a drag-and-drop workflow interface, the capability allows administrators to easily assemble and adjust workflow for steps such as registration, authentication, authorization, and more. This capability means users will receive highly tailored and personalized customer experiences across channels and brands. **This capability accelerates digital agility and reduces costs.**
Orchestration	How does the vendor pre-identify a user's digital signal such as location, IP address, device type, operating system, browser type, and more before a username is even collected?	No-code/low-code identity orchestration also gives administrators the ability to build authentication workflows that easily configure, measure, and adjust user login journeys using a wide array of contextual signals. Administrators can also quickly consume out-of-the-box authenticators, utilize existing authenticators, and integrate with cyber security solutions. **This capability strengthens security.**
Single Sign-On (SSO)	Does the vendor provide federated SSO capabilities?	Your customers expect to have access to all of your applications without having to remember unique credentials for each one. Give them what they want by providing a consistent and convenient login experience with federated SSO. **This capability strengthens security and enhances customer experience.**

Capability	Evaluation Criteria	Why It Matters
Progressive profiling	Does the vendor support progressive profiling?	Rather than asking your users to fill out extensive registration forms, you can implement progressive profiling, a technique to collect user information as users interact with your system, on your website or application. For example, you might collect just the user's name, email, and password on the initial sign up. At a later point in time, you might ask for the name of their company and their title. **This capability reduces prospect abandonment.**
Account Recovery	Does the vendor provide account recovery and easy-to-use password policies?	Most customers will forget their passwords at some point. Provide a secure and simple account recovery process by using password reset best practices and centralized password policies. **This capability strengthens security posture and enhances customer experience.**
Multi-Factor Authentication (MFA)	Does the vendor support multiple forms of MFA?	You need to give your customers convenient options that make it easy for them to use MFA so everyone can reap the security benefits. Vendors should support methods like SMS and email OTPs, soft tokens, FIDO, and more. **This capability strengthens security posture and enhances customer experience.**
Passwordless	Does the vendor support the FIDO standard?	FIDO allows customers to leverage credentials stored on a trusted device. It's a very convenient and secure standard that's growing in use and can ultimately replace passwords entirely. **This capability strengthens security posture and enhances customer experience.**
Risk-based authentication	Does the vendor support risk-based authentication policies?	No matter how convenient you make MFA, it still adds friction. Intelligent policies that allow you to step MFA requirements up or down depending on risk introduce friction only when the request warrants it. **This capability strengthens security posture and enhances customer experience.**

Capability	Evaluation Criteria	Why It Matters
Identity verification	Does the vendor provide native or third-party identity verification to enable KYC/identity proofing and customer checks post-login?	Deepfakes and AI-generated impersonation is becoming more sophisticated and difficult to detect and prevent. At the same time, onerous identity verification can cause unnecessary friction and increase the risk of abandonment. Identity verification helps organizations combat risks while reducing unnecessary friction at onboarding, call center, and hybrid channel touchpoints. **This capability strengthens security posture and enhances customer experience.**

> “We needed a solution that allowed for secure and quick onboarding of new customers and businesses with an exceptional digital experience throughout the customer lifecycle. Ping Identity could provide the highest level of security as well as the flexibility we required to deliver the services our customers need.
>
> – Joko Kurniawan, SVP of IT Digital Service Enablement, BTPN Bank (read full story).

Fraud Prevention and Security

The criteria in this section focus on detecting, responding to, and preventing fraud at all stages of the customer journey, as well as protecting customer data and mission-critical infrastructure from malicious actors.

Capability	Evaluation Criteria	Why It Matters
Fraud detection	Does the vendor provide online fraud detection?	The fraud landscape continues to grow exponentially across financial services. Fraud detection is more important than ever. Ask your vendor if they can detect identity fraud threats in real time, identifying attempts at account takeover, session hijacking, new account fraud, synthetic identity fraud, automated attacks, and more. **This capability strengthens security.**
Fraud detection - account take over (ATO)	Does the solution detect ATO attacks?	ATO occurs when a bad actor gains unauthorized access to a user's digital identity account, and is often the source of data breaches, theft, and other fraudulent activities that lead to lost revenue, damaged brand reputation, and significant mitigation costs. **This capability strengthens security.**
Fraud detection - new account fraud (NAF)	Does the solution detect NAF?	NAF occurs when a bad actor creates a new account with malicious intent. These new accounts may be used to test stolen payment information, make fraudulent applications for credit, and other fraudulent activities that lead to lost revenue, damaged brand reputation, and significant mitigation costs. **This capability strengthens security.**
Fraud detection - malicious bots	Does the solution detect malicious bots and other automated attacks?	47% of internet traffic today is bots, and they can be used to perpetrate fraud at scale. To stop password spraying, brute force attacks, sniping, fraudulent new account creation at scale, card testing, and more, you need a solution that can accurately distinguish between human and non-human users. **This capability strengthens security.**
Fraud prevention - synthetic identity and deepfakes	Does the solution protect against synthetic and stolen identity fraud and deepfakes?	Financial service providers continue to suffer high rates of deepfake, adversarial-AI, and identity fraud attacks.. Your organization needs an AI-enabled solution that can accurately identify users and stop these identity crimes in an era where human eyes and ears can no longer accurately distinguish what is real in the digital sphere. **This capability strengthens security.**

Capability	Evaluation Criteria	Why It Matters
Fraud prevention - composite risk scoring	Does the solution pull together fraud and risk signals from multiple sources and tools, and provide composite risk scoring?	Most financial service providers have use multiple solutions to leverage risk signals that can be used to evaluate the riskiness of a user or session, but these tools rarely talk to each other. You need a solution that can bring all of these sources of context into a single, real-time decision, delivering a composite risk score based on your organization's unique requirements, so that you can respond appropriately to the level and type of threat. **This capability strengthens security.**
Fraud prevention - authentication	Does the vendor support risk-based authentication policies?	No matter how convenient you make MFA, it still adds friction. Dynamic access policies that take real-time risk into account allow you to adjust authentication requirements up or down, introducing friction only when the request warrants it and letting safe users stay logged in longer. **This capability strengthens security.**
Fraud prevention - customer journey	Does the solution monitor and protect the entire customer journey, invoking additional security measures at any point in the user session when risk is high?	Most identity solutions only protect at the initial authentication; however, this approach means the context collected throughout the rest of the customer journey is not taken into account when evaluating risk. Organizations need fraud prevention solutions that measure risk continuously, so that it is possible to stop cyber criminals as they attempt to perform other activities beyond authentication. **This capability strengthens security.**
Fraud mitigation	Does the vendor support a variety of fraud mitigation methods to be deployed based on the level and type of risk?	Many fraud vendors stop at detection. You need a solution that can evaluate the threat signals coming in from fraud detection tools, make a decision in real time, and initiate fraud mitigation. **This capability strengthens security.**
Dynamic authorization	What types of authorization methods and access controls are offered by the vendor?	Dynamic authorization is the function of determining if a user has permission to access a specified resource(s), such as a website(s), record(s), or document(s), by using policy-based logic, entitlements, and context to prohibit unauthorized parties from accessing customer data and mission-critical infrastructure. **This capability strengthens security.**

Capability	Evaluation Criteria	Why It Matters
Encryption	Does the vendor's identity store encrypt data both at rest and in transit?	Identity data must be encrypted both at rest and in transit to ensure maximum security. Best practices also recommend using an embeddable repository that enables seamless sharing of real-time customer, device, and user identity data across various environments. From a hosting perspective, the identity store should offer high availability, robust performance, and top-tier security. Additionally, it should be fully compliant with LDAP v3 and integrate effortlessly with any directory. **This capability strengthens security and compliance.**
API security	Does the vendor provide standards-based API security?	Standards-based API security is crucial in financial services to ensure secure and seamless data exchange while complying with strict regulatory requirements. Frameworks like OAuth 2.0, OpenID Connect (OIDC), and JWT-based access control provide robust authentication, authorization, and identity management, protecting sensitive financial data from unauthorized access and fraud. **This capability strengthens standards compliance and security.**
Edge security for legacy applications	Does the vendor provide the ability to connect and extend to legacy systems and applications through edge security?	Many organizations rely on a multitude of legacy systems and applications that store customer data and credentials but often lack built-in features for user registration, authentication, authorization, or federation. Consequently, the ability to connect and extend these legacy systems with a modern identity system is a crucial feature of CIAM platforms. This is achieved through an identity gateway, which enables seamless and secure communication between legacy and contemporary systems and applications. **This capability strengthens customer experience, performance, and security.**

Own Your Customer Identity Strategy

Discover the questions you MUST ask when evaluating CIAM vendors for Financial Services.

Get the RFP Workbook

Capability	Evaluation Criteria	Why It Matters
Edge security	Does the solution use edge controllers to secure IoT identities and their associated credentials to be trusted and usable across numerous connected ecosystems to prevent man-in-the-middle and other types of attacks?	Most IoT devices are not secure. Identity at the edge secures devices and the data they collect with edge controllers and identity message brokers. Edge controllers secure IoT identities and their associated credentials to be trusted and usable across numerous connected ecosystems to prevent man-in-the-middle and other types of attacks. **This capability strengthens security.**
Passwordless	Can the vendor's passwordless authentication solution be used for both initial login and step-up authentication, including transactional authorization?	Creating passwords that rely on personal information makes accounts vulnerable to attacks. Using a password management system is one way to deal with the password problem, but some of these services themselves are vulnerable. Passwordless authentication reduces an organization's attack surface by virtually eliminating credential theft arising from phishing attacks, password reuse, credential stuffing, keyloggers, and more. **This capability strengthens security.**
Privacy	Can the vendor enforce customer consent?	Many identity vendors focus solely on how they collect consent, leaving the responsibility of enforcing it to disparate application teams. This approach can lead to inconsistencies and added complexity, especially for large or growing organizations. To ensure consistent and effective consent management, it's crucial to have the ability to centrally enforce consent across all systems and applications. **This capability enables customer trust.**
API security	Does the vendor provide deep insights into API traffic to detect potential threats?	Every application relies on APIs that can be vulnerable to exploitation and breaches. To protect your organization, you need a CIAM solution that continuously monitors all API traffic, detecting potentially malicious behavior and preventing attacks before they can cause harm. **This capability strengthens security.**

Capability	Evaluation Criteria	Why It Matters
Risk-based access	Does the vendor utilize contextual authentication and authorization factors during a session to assess risk, only triggering stronger authentication mechanisms when necessary by evaluating the user's identity and context?	To ensure the continuous authenticity of users, devices, 'things', and services, and to mitigate risk whenever anomalies are detected—even during active sessions—contextual access should be employed. Contextual access incorporates context-based intelligence into policies, assessing risk and safeguarding resources both at the time of access and throughout a digital session. By applying fine-grained authorization policies, adaptive risk assessment, multi-factor authentication, and push authorization, it strengthens security without burdening users, invoking stronger authentication mechanisms only when necessary. **This capability strengthens security.**
AI/ML threat detection and prevention	Does the vendor offer a threat detection solution that leverages artificial intelligence (AI) and machine learning (ML)?	Cybercriminals are becoming more sophisticated, leading to an increase in cyber threats, such as account takeovers. Account takeover (ATO) occurs when a bad actor gains unauthorized access to a user's digital identity account. ATO is often the source of data breaches, theft, and other fraudulent activities that lead to lost revenue, damaged brand reputation, and significant mitigation costs. To provide legitimate customers with the seamless, secure access experiences they demand, enterprise organizations require a modern security solution that removes unwanted friction while strengthening security. An AI and ML-powered threat protection solution helps to prevent account takeover and fraud at the identity perimeter. **This capability strengthens security.**
Zero Trust security	Does the solution provide a Zero Trust Security and CARTA model of risk and/or value-based authentication, enabling users, devices, things, and applications to have different levels of credentials to authenticate against a common Identity store?	CIAM platforms should be able to determine whether an entity requesting an action is authorized to do so, and if they have proven they are the entity they claim to be with a sufficient level of assurance based on the risk of the specific action. Within a Zero Trust Security model, every action taken must be properly authenticated and authorized. To do this, authentication and authorization decisions leverage contextual information and become risk-based rather than binary, taking into consideration a rich set of information. **This capability strengthens security.**

Capability	Evaluation Criteria	Why It Matters
Least privileged access	Can the vendor enable the principle of least privileged access to only grant access that is essential to perform an intended purpose?	Scopes enable the principle of ‘least privileged access’. This means only granting access that is essential to perform an intended purpose. A first step towards achieving this fine-grained authorization is developing a mechanism to 'distribute' and assign strongly typed scopes to applications, API endpoints, and other protected resources. Scopes must then be coupled with real-time context at policy-enforcing gates throughout the identity ecosystem. Scopes for fine-grained, actionable rules that can be used to make authorization decisions should also be applied. **This capability strengthens security.**
Secure transactions	Does the solution support secure online transactions (such as "cardholder not present" security flows)?	By leveraging fine-grained authorization capabilities, organizations can effectively enable complex online transactions, such as "cardholder not present" security flows, when a bank card is not present. This allows organizations to mitigate risks across multiple customer-initiated transactions without introducing undue customer friction. **This capability strengthens security and enhances customer experience.**

> Risks and threats are constantly evolving in our space. Ping simplifies the authentication experience for our end users while innovating to provide the security we need.
>
> – Sebastiaan Gybels, VP of Information Security, Next Capital Group (read full story).

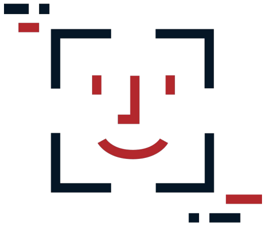
Customer Experience

The criteria in this section focus on the many ways in which CIAM helps financial services providers enhance customer experiences across all touchpoints and channels of interaction, while enabling digital innovation:

Capability	Evaluation Criteria	Why It Matters
Orchestration	Does the solution allow access journeys to be easily created, viewed, and changed with no-code/low-code drag-and-drop user interfaces?	To provide secure, effortless customer journeys, a CIAM solution should provide financial service providers with no-code/low-code identity orchestration capabilities. With a drag-and-drop workflow interface, administrators can easily assemble and adjust workflow steps for all access journeys. This capability means users will receive highly tailored and personalized customer experiences across channels and brands. **This capability accelerates digital agility and reduces costs.**
Access journey analytics	Does the vendor enable login evaluations that provide abandonment insights?	To continuously improve and secure the customer journey, data-driven insights are essential. As part of identity orchestration, user login analytics provide metrics and timers to analyze end-user interactions and their devices across all channels and business lines. These platforms should empower administrators to optimize the customer journey by using contextual and behavioral analytics to examine factors like devices and browsers used, login locations, and the duration of login processes across the user base. **This capability strengthens customer journeys through advanced data.**
Identity lifecycle management	Does the vendor provide real-time, bidirectional synchronization capabilities?	Real-time, bidirectional data synchronization lets you consolidate disparate identity silos to create a unified profile. It also reduces mitigation risks and prevents downtime. **This capability strengthens customer experience and drives revenue.**
Identity relationship management - organizational hierarchies	How does the CIAM solution support unique IAM configurations for different hierarchies or lines of business (LOBs)?	Most enterprise financial service providers create a hierarchy of departments or LOBs to fit their needs around how they structure their business. These hierarchies inform how they then delegate administration, as well as access rights to users within those organizations. The hierarchical, multi-brand, and complex organization design feature gives enterprises the flexibility to set up unique identity and access management configurations, like password policies and access permissions, for different audiences. **This capability enables cross-organizational CIAM distribution.**

Capability	Evaluation Criteria	Why It Matters
Identity relationship management - modelling	Does the vendor provide identity relationship modeling at a granular level for identity management between those relationships?	To create secure, personalized, omnichannel experiences, CIAM providers must allow financial service providers to aggregate relational data between users and entities to create a highly comprehensive, single view of the customer. This is achieved by establishing a common customer data model, connecting a broad range of data sources, implementing simple synchronization and reconciliation logic, and allowing access to customer data in an appropriate format. **This capability strengthens customer experience and drives revenue.**
Single view of identity	Does the vendor enable integration with third-party systems to consolidate identity data silos to create a single view of the customer organization-wide?	A single view of a customer (an identity) organization-wide improves security, customer service, marketing initiatives, and more. For CIAM platforms to support a unified view of identities, they must have the ability to integrate with other systems and consolidate multiple customer data silos to create a single view of an identity organization-wide. **This capability fosters integration and improves overall operations.**
MFA / software development kit (SDK)	Does the vendor embed MFA in your own mobile app?	Boost security for your customers by turning your mobile app into a second authentication factor using secure push notifications. They're more convenient and secure than many other forms of MFA. **This capability adds security without sacrificing ease-of-access.**
Personalization	Does the CIAM platform include flexible hosted user interface (UI) options?	Financial service providers with multiple brands must recognize each user and provide a personalized experience, guiding them to the appropriately branded access point. In multi-party ecosystems, organizations need to manage different business units or user groups separately within their identity hierarchy, sometimes extending certain privileges to partners to better manage their end customers, also referred to as business-to-business-to-consumer (B2B2C). A robust CIAM solution should offer multi-brand UI theming, allowing organizations to create tailored customer journeys that align with the appropriate brand. **This capability strengthens customer experience and drives revenue.**
Impersonation	Does the vendor support OAuth 2.0 token exchange, including a CIBA (client-initiated backchannel authentication) grant?	Organizational representatives, like call center staff, may occasionally need to "impersonate" a user to take defined action on their behalf. A secure impersonation feature allows users to grant temporary control of their account to another party for a specified period. Extending consumer digital services to third parties requires support for OAuth 2.0 token exchange. **This capability ensures your security can address emerging threats.**

Capability	Evaluation Criteria	Why It Matters
Self-Service	Does the vendor provide account recovery and easy-to-use password policies?	Most customers will forget their passwords at some point. Providing a secure and simple account recovery process by using password reset best practices and centralized password policies improves customer experience and reduces call center costs. **This capability strengthens security and customer experience.**
Privacy	Does the vendor enable users to have visibility into, and control of, their consent and privacy settings?	By giving customers the ability to control who and when their data is shared with third parties, organizations can achieve regulatory compliance with privacy regulations (such as the GDPR), while building long-lasting customer trust and loyalty needed to maximize lifetime value. **This capability ensures compliance and adapt to evolving regulations.**



Own Your Customer Identity Strategy

Discover the questions you MUST ask when evaluating CIAM vendors.

Get the RFP Workbook

Regulatory Compliance

The criteria in this section focus on the many ways in which CIAM helps financial services organizations achieve compliance with information security, digital operational resilience, API, payments, data residency, and privacy regulations.

Capability	Evaluation Criteria	Why It Matters
Open standards	Does the vendor support both basic and advanced open standards, including OAuth2, OpenID Connect, SAML,OAuth2, UMA 2.0, Device Flow and OAuth 2.0 Proof-of-Possession, FIDO2, WebAuthN, and Client-Initiated Backchannel Authentication (CIBA)?	Open standards are established technical norms that developers use to ensure consistent capabilities and functionality across systems. Identity security is fundamentally built on standards like OAuth2, OpenID Connect, and SAML. However, leading digital identity providers are going beyond these core standards to support emerging trends by integrating advanced protocols. For example, UMA 2.0 enables users to securely share access to personal data with third parties. Other advanced standards include OAuth 2.0 Proof-of-Possession, which ensures that the bearer of a token is its legitimate owner, and OAuth2 Device Flow, designed for client devices with limited user interfaces. **This capability strengthens security and compliance.**
Data sovereignty	How does the vendor solution deliver granular data sovereignty?	Security concerns, like data sharing and data sovereignty, have created challenges for financial service providers seeking to embrace SaaS-based CIAM solutions. Traditional SaaS vendors often use multi-tenant architectures that combine multiple customers (tenants) into a single instance, increasing the risk that one organization's actions could affect others. To address these concerns, the ideal CIAM SaaS platform should offer full tenant isolation, ensuring that data and workloads are completely separate. This isolation not only reduces risks but also simplifies scaling and storing sensitive identity data in the cloud. **This capability strengthens security and compliance.**
Scale and performance - extreme scale	Does the vendor handle extreme scale and performance and have a track record of success to support it?	If your unified profile can't scale, it risks going down, leaving customers unable to sign in or access their data. Vendors should be capable of supporting hundreds of millions of stored identities and billions of attributes, even during peak usage with hundreds of thousands of concurrent users. To ensure they can meet customer needs, they should also provide references that confirm high availability and low latency during peak demand periods. **This capability strengthens performance and security.**

Capability	Evaluation Criteria	Why It Matters
Scale and performance - peak demand	Can the vendor scale their identity registration, authentication, and authorization services by several orders of magnitude to handle both anticipated peaks, like those during high-profile events, and unexpected surges?	Scale, performance, and availability are critical non-functional CIAM requirements because if the identity platform goes down, so will the business. CIAM providers should support both 'service availability' and 'session availability'. Service availability ensures users can access a site when a server goes down. Session availability preserves and keeps a session running if a server goes down. CIAM providers should also support a variety of scale scenarios. This includes a shifting number (often in the millions) of users, devices, and things that need to be stored in a database, as well as changing frequencies and lengths of simultaneous and concurrent sessions. **This capability strengthens customer experience, performance, and security.**
Data residency	Does the vendor offer flexible data residency?	Data residency and data sovereignty are crucial concepts that govern where user data is stored and the legal authority that applies to it, regardless of location. Data residency typically requires that a user's data be collected, stored, and processed within their country's borders. To comply with regulations like GDPR, CIAM providers should offer flexible data residency options, enabling privacy-bound data storage and fractional replication of personal data across data centers in multiple jurisdictions. This ensures that user data can be processed in a way that is sensitive to the legal and regulatory requirements of specific regions. **This capability strengthens security, performance, and compliance.**
Privacy - auditable consent	Can the vendor collect and store auditable consent records?	When collecting customer consent, you must collect the data in an auditable way. Your CIAM vendor should be able to store the time the data was collected, evidence of collection (such as an IP address), and other information needed for privacy audits. **This capability strengthens compliance and enables customer trust.**
Privacy - UMA 2.0	Does the vendor support privacy and consent framework based on the UMA 2.0 standard?	Privacy regulations like GDPR require that users have control over their personal data, including privacy, security, and usage preferences. To ensure global and regional compliance, CIAM platforms must incorporate Privacy by Design principles and consent mechanisms based on the UMA 2.0 standard. They should also integrate with other tools that help meet regulatory requirements. These mechanisms should offer users fine-grained control to manage and audit data related to themselves, their devices, and their 'things.' Equally important is that the user interface for these privacy and control features is intuitive and user-friendly. **This capability builds customer trust.**

Capability	Evaluation Criteria	Why It Matters
Privacy - fine-grained authorization	Does the vendor support fine-grained dynamic authorization to meet privacy regulations?	Privacy regulations are diverse and can vary by organization, industry, geography, and more. CIAM solutions should contain centrally managed privacy policies that let you enforce customer consent and govern data sharing on an attribute-by-attribute level to every application. **This capability strengthens compliance and enables customer trust.**
Federation standards	Does the vendor offer federated single sign-on based on open standards such as OAuth, WS-Federation, WS-Trust, OIDC and SAML?	Federated SSO allows users, like partners, to securely access multiple organizations' web properties and applications using a single account. This trusted system is based on federated relationships between organizations and enables SSO by passing authentication tokens between their identity providers. Federated SSO relies on open standards like OAuth, WS-Federation, WS-Trust, OpenID Connect, and SAML to facilitate secure authentication across different organizations. **This capability strengthens compliance.**
IAM auditing	Does the vendor enable auditing for system security, troubleshooting, usage analytics, and regulatory compliance?	System auditing and analytics capabilities are mission-critical functions. CIAM platforms must be able to conduct audits for system security, troubleshooting, usage analytics, and regulatory compliance. Audit logs ought to gather operational information about events occurring within a deployment to track processes and security data, including authentication mechanisms, system access, user and administrator activity, error messages, and configuration changes. **This capability strengthens compliance.**
KYC, AML, and open banking	Does the vendor support the identity, authentication, consent, and fine-grained authorization requirements mandated by PSD2 regulations, Open Banking specifications, and KYC/AML requirements?	PSD2 (and soon-to-be PSR1/PSD3), privacy, and open banking requirements continue to evolve rapidly across most parts of the world. To enable organizations to meet regulatory requirements and maximize ROI on open banking and open finance investments requires modern customer identity and access management (CIAM) solutions that include comprehensive fine-grained authorization capabilities. **This capability strengthens compliance, accelerates revenue, and reduces costs.**

Capability	Evaluation Criteria	Why It Matters
FAPI conformance	Does the vendor conform with the OpenID Foundation Financial Grade API (FAPI) 2.0 certification?	Financial services organizations looking to advance their open banking offerings need to ensure the external APIs that allow applications to access customers' financial accounts, data stored therein, and privacy settings are secured and compliant with industry standards. FAPI 2.0 specifications provide the basis for doing so. **This capability strengthens compliance, accelerates revenue, and reduces costs.**
Strong customer authentication	How does the vendor support authentication, authorization, open banking strong customer authentication (SCA), and fine-grained authorization (transaction flows)?	Open banking providers need to provide customers with a wide range of SCA options to introduce the appropriate amount of friction/security needed to protect customer data. Higher assurance of verification can also be required to complete high-value transactions. **This capability strengthens security, customer experience, and compliance.**

> As we move into new regions like the U.S., we don’t have the time or budget to rewrite every app to meet each country’s privacy requirements. We also want to be able to quickly add new features like social login and configure them on the fly. Most identity solutions require extensive programming to make these changes. But Ping Identity’s orchestration capabilities allow us to make changes in a low code manner. Its easy-to-use drag-and-drop interface allows us to create customizable and secure customer journeys, allowing us to quickly enter new markets just as we recently did in the U.S.
> – Ashwini Kumar, Senior Engineering Manager, Mobile Premier League

Implementation and Operational Considerations

The criteria in this section focus on CIAM deployment options, migration, performance, and resiliency at scale ensuring that financial services organizations can deliver value to their end-users at pace.

Capability	Evaluation Criteria	Why It Matters
API-first model	Does the provider use an API-first development model to create one common REST API framework across the entire platform?	The API First Model is a developer-centric method of creating a solution. Within this model, a provider first creates the API and then builds the platform around it. This results in less complexity for external developers and organizations. For ease of use, scalability, and flexibility, digital identity providers should apply this API first development model to create one common REST API framework across the entire platform to provide a single, common method to invoke any identity service. The result should be a simple and secure way to extend identity to all realms, including social, mobile, cloud, and IoT. **This capability drives revenue.**
Non-standard app support	Can the vendor connect to custom applications that are not standard-based?	While your platform must support standards, many of your customer-facing applications may not. Your vendor should be able to connect to these applications and provide simple access to any digital properties in your portfolio. **This capability accelerates agility and reduces costs.**
Partner ecosystem	Does the provider have a strong ecosystem of respected consultancy, technology, and integration partners?	The strongest CIAM solutions are those that work well with a wide variety of other technologies, software, and industry leaders to solve the unique goals of each organization. As such, CIAM providers must have a strong ecosystem of respected consultancy, technology, and integration partners. This ecosystem should include pre-built, tested, and always updated integrations ready to be easily utilized. **This capability accelerates agility, reduces costs, and drives revenue.**
Administrator experience - best practices	Does the vendor provide best practices, sample apps, and out-of-the-box UIs?	You need to deliver secure and seamless experiences for your customers. CIAM vendors should make this easier by providing tools and resources to ensure your success, including extensive API documentation, sample apps, and out-of-the-box integration kits to get you up and running quickly. **This capability accelerates agility, reduces costs, and drives revenue.**

Capability	Evaluation Criteria	Why It Matters
Administrator experience - legacy protocols	Does the vendor enable applications to access to the customer profile with REST APIs?	Legacy protocols like LDAP are necessary for communicating with legacy directories to create a unified profile, but modern apps prefer APIs when accessing customer data. A unified profile should provide those APIs. **This capability accelerates agility.**
Deployment flexibility - deployment model	Does the vendor support multiple deployment options?	You should be able to choose where to deploy customer identity to meet your specific business needs. A CIAM vendor should be able to provide you with deployment options, including the simplicity of a multi-tenant SaaS solution, the configurability of a single-tenant managed solution, or the customizability of an on-premises solution. **This capability accelerates agility, reduces costs, and drives revenue.**
Deployment flexibility IDaaS	Does the vendor offer both multi-tenant and single-tenant Identity-as-a-Service (IDaaS) deployment options?	Many financial service providers are prioritizing deployments in clouds that are managed for them. If yours is one of them, you need a vendor that offers IDaaS deployment options that suit your needs, whether that's multi-tenant or private-tenant IDaaS to give you the control you need over your environment. **This capability accelerates agility, reduces costs, and strengthens security.**
Deployment flexibility - DevOps	Does the vendor support containerization and orchestration for DevOps?	Some organizations want to maintain full control over their identity solution by managing identity in an environment they fully control (whether that's a private cloud or self-managed). If either of these apply, be sure your vendor can support your preference. **This capability accelerates agility, reduces costs, and strengthens security.**
Deployment flexibility - any cloud	Can the solution be deployed within any cloud environment, including multi-cloud, bring-your-own-cloud, or hybrid cloud?	CIAM platforms should include flexible consumption options that include multi-cloud and hybrid-cloud deployments. Multi-cloud environments have become popular due to their increased flexibility, availability, and scalability. These environments allow financial service providers to eliminate vendor lock-in and speed time-to-market while reducing complexity and saving time and money. Hybrid environments include both on-premise and cloud environments. Cloud environments support needs at scale, while on-premises environments are advised to store sensitive data for better security. **This capability accelerates agility, reduces costs, and strengthens security.**

Capability	Evaluation Criteria	Why It Matters
Migration	Does the vendor support co-existing with legacy systems to enable you to do a phased migration to a modern CIAM solution?	For most organizations, it usually isn't feasible to take a rip-and-replace approach when moving from a legacy system to a modern CIAM solution. When your vendor can support a phased migration approach by allowing the legacy and modern systems to co-exist, you'll greatly minimize the potential for downtime and other risks. **This capability accelerates agility, reduces costs, and strengthens security.**

> In the trillion-dollar mortgage industry, technology is a competitive differentiator. The interoperability and speed we gain with Ping Identity give us the agility we need in business.
>
> – Vincent ten Krooden, Head of Technology, Mortgage Choice (read full story).

Evaluating Vendors & Solutions

After you've defined your evaluation criteria, you'll want to organize them in a way that makes it easy to evaluate how your shortlist of vendors stack up. You may want to use a Google Sheet or Excel spreadsheet for this. We suggest first creating rows for each of your evaluation criteria. Next, add columns for each vendor you want to evaluate. Then you can rate each vendor on how well they meet your criteria using a point-based rating system like this:

0 = Does not meet requirement
1 = Very limited support for requirement
2 = Partially meets requirement
3 = Meets or exceed requirement

Where to Go From Here

Choosing a customer identity solution is an important decision. The first step is identifying your organization's critical objectives and measures of success. Then you can apply your understanding of customer identity capabilities as detailed throughout this guide to ensure you prioritize vendor solutions that meet your specific requirements.

Ready to take the next step?

Get the RFP Workbook to unlock the critical questions you need to make the right choice.

Try our all-in-one platform for free.

Contact us directly to schedule a conversation.

> “Providing a secure, scalable portal with unified identity and access management is a key part of our business strategy and has helped Utah maintain its top ranking for business friendliness. It's probably the most critical piece of our enterprise architecture.
>
> – Dave Fletcher, Chief Technology Officer, State of Utah

Hear From the Experts:

- Gartner® Magic Quadrant™: Access Management, 2024
- Gartner Critical Capabilities: Access Management, 2025
- KuppingerCole Leadership Compass: CIAM, 2024
- KuppingerCole Leadership Compass: Identity Fabrics, 2024
- Forrester Wave: CIAM, 2024

Disclaimer: Gartner, Predicts 2024: The Changing Role of the Identity and Access Management Leader, 1 December 2023, Michael Kelley, Rebecca Archambault, Nathan Harris, Henrique Teixeira, Oscar Isaka GARTNER is a registered trademark and service mark, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

#4007 | 02.25 | v03