datos INSIGHTS

March 2024

Identity Beyond the Feature: Strategic Investments for Financial Services

John Horn

This report provided compliments of:

okta

March 2024

Identity Beyond the Feature: Strategic Investments for Financial Services

John Horn

Table of Contents

List of Figures

List of Tables

Summary and Key Findings

For many financial institutions (FIs), insurers, and the financial service firms supporting them, improved authentication and identity capabilities are often driven by user-facing *feature* enhancements. These user-facing methods commonly operate in the multifactor authentication (MFA) and risk-based authentication (RBA) categories. Much has been written about these features in terms of effectiveness, consumer vs. workforce flows, how cybercriminals can bypass underlying technology, and regulatory requirements. More modern authentication features include biometric MFA and a new class of solutions called phishing-resistant MFA.[1] Modern authentication features tend to specify the kind of identity claim that must be present (or in some cases, not present) to meet current security and regulatory requirements.

Features are obviously important, but this advisor has long observed firms becoming overly engrossed in feature improvements while losing traction against critical identity framework (nonfeature) capabilities. The complexity of the identity vendor choices plus cybersecurity personnel talent gaps can combine to make it more difficult to understand identity framework improvements, formulate business cases, and win investment. Complicating matters further are lines-of-business leaders. They tend to prioritize feature improvements, which directly impact the customer and thus are more practical to understand.

But what if the outcomes most desired by business and risk leadership are best achieved through identity framework investments rather than chasing technological "silver bullets" with the most features? What are these strategic outcomes, and what does the business need from modern identity solutions to achieve these outcomes? Are there products in the market that represent these strategic patterns, or must CISOs and other leaders wait until they arrive at some future point? This report provides an analysis of the underlying problems at FIs and insurers and presents a business/functional vision for how CISOs and other financial services leaders should view strategic identity framework investments to transform their businesses. The key findings for this report follow:

[1] "Implementing Phishing-Resistant MFA," U.S. Cybersecurity & Infrastructure Security Agency (CISA), October 2022, accessed February 21, 2024, https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf.

- **Business vision for transformative identity is often stuck in the clouds:** High-level principles and slideware from industry leaders do not translate well into actionable plans for financial services firms. Vendor-supplied business visions are often biased toward the vendor's own products.
- **At most financial services firms, few domain experts exist for transformative identity:** Within many FIs and insurers, deep identity talent has been lacking for years. Identity talent gaps are more severe than cyber talent shortfalls. Seasoned identity professionals exist, but they are rare, creating difficult challenges for businesses. Senior talent is also lacking at some market vendors, including some identity providers.
- **At most financial services firms, transformative identity requires steady multiyear executive sponsorship:** Implementing identity improvements while operating the business is akin to changing the tires on a moving car. Most institutions will need multiple projects spanning budget cycles. Executive champions and program leadership are critical to achieving strategic business outcomes over the next three to four years.
- **CISOs are trending as strong budget holders for identity solutions:** Historically, identity buyers at FIs have been CIOs (for customer identity, aka CIAM) and CISOs (for workforce or enterprise identity). However, Datos Insights' research in 2023 indicates CISOs function as CIAM budget holders for 24% of FIs, second only to CIOs as CIAM budget holders at 36% of FIs. Many executive stakeholders exist for identity-related decisions, especially on the customer/CIAM side of the business.
- **For the past two years, workforce identity/security improvement has been the top stated CISO priority from U.S.-based FIs and insurers:** Datos Insights' cyber executive councils for FIs and insurers continue to assert workforce identity and security modernization efforts as top priorities. Stakeholder relationships, tech debt, and the number of solutions involved are cited as reasons for businesses' multiyear improvement journeys. CISOs are making year-over-year progress.
- **Lack of U.S. public sector identity standards hurts financial services identity leaders:** The federal government continues to lack a champion and investment to encourage citizens toward using digital forms of identity such as mobile driver's licenses (mDLs). Without this citizen and societal transition, FIs and insurers face additional headwinds in deploying modern identity features such as passkeys.

- **"Identity" has become an oversubscribed term with different meanings based on context, vendor, and speaker. Meet the new needed term: intent.** Alongside authentication and identity, *intent* will enable experts to collaboratively design new solutions the market needs and help business leaders to understand them.

Introduction

Claims-based identity is a common way for applications to acquire the identity data they need about users, then abstract identity and access control into two parts: a notion of claims data and the concept of an issuer or an authority.[2] Claims-based identity supports the broad function of *identification*, how users and systems properly identify themselves to other parties. As the digital ecosystem has evolved over the past three decades, the term *identity* has been closely coupled with the function of *authentication*, defined as the processes and methods by which identity claims are validated.

Several classes of authentication solutions exist in the market to validate real (human) identity claims, digital identity claims, and the important connection between digital and human identity claims. Solutions operate within the established category of identity and access management (IAM), which reflects identity's historical foundation and conceptual basis. Providers and practitioners tend to think of identity under the umbrella of IAM and risk management under the responsibility of CISOs. Knowledge-based identity claims, such as passwords and other shared secrets, have served the market for years.

Today, identity is a key aspect of heightened business risk for financial services. Due to cyberattacks and data breaches in the past decade, commonly used shared secrets are no longer secret. Data breaches have exposed credentials supporting human identity, such as Social Security numbers. It is estimated at least half of all adults in the U.S. have had their Social Security number compromised.[3] Data breaches have exposed billions of user identities and passwords, the most common form of identity claim supporting digital authentication.

In 2023, cyberattacks resulted in 2,365 breaches worldwide, impacting an estimated 343,338,964 victims.[4] User passwords are no longer fit for purpose in financial services and many other industries. Strategically, at the same time, market providers have delivered major technical advances in identity solutions. FI and insurer business leaders may have little interest in identity, but they are extremely interested in what identity can now

---

[2] Dominick Baier, Vittorio Bertocci, Keith Brown, Scott Densmore, Eugenio Pace, and Matias Woloski, "A Guide to Claims-Based Identity and Access Control," Microsoft, 2011, accessed February 21, 2024, https://download.microsoft.com/download/F/1/4/F1475A9B-5AD3-4B54-B16D-8B34CD416159/Claims-based%20Identity%20Second%20Edition%20device.pdf.

[3] Better Identity Coalition, "Identity, Authentication and the Road Ahead," January 25, 2023.

[4] Identity Theft Resource Center (ITRC), "Identity, Authentication and the Road Ahead," January 25, 2023.

enable—greater business agility and a more operationally mature enterprise with stronger security assurance.

This report is intended for CISOs, CIOs, CTOs, and chief identity officers charged with transforming and securing their digital business. The success of financial services and the enterprise is at stake.

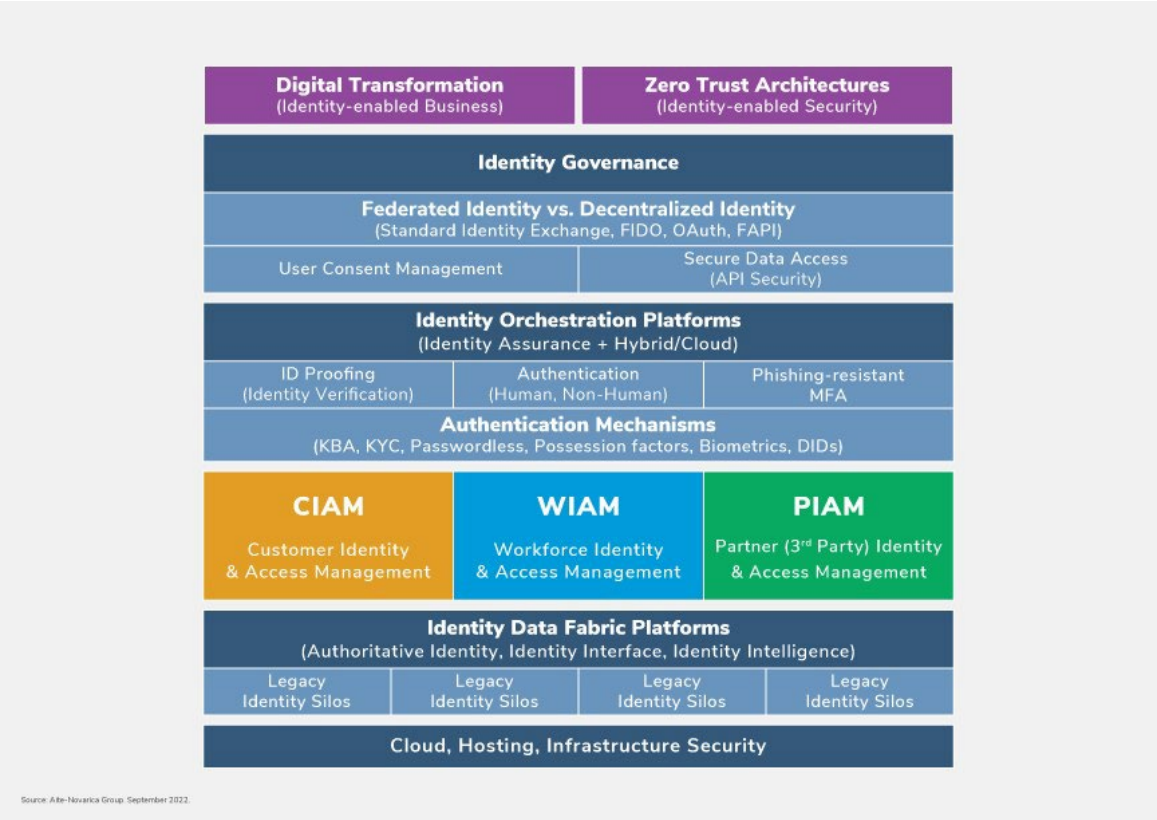
Methodology

This report leverages the Datos Insights' identity taxonomy launched in 2022, describing modern identity capabilities and opportunities in the market, as well as two 2023 Datos Insights research reports with high emphasis on digital identity. It also includes 2023 survey results and discussions with the Datos Insights' FI Cyber Executive Council and Insurer Cyber Executive Council in February and May of 2023. This report includes insights from a separate 2023 Datos Insights quantitative survey of 100 FIs regarding digital identity modernization. Finally, this report is supported by strategic discussions with four market-leader providers that announced transformational capabilities during the second half of 2023 that align with the outcomes described in this report.

Identity Investment Observations and Strategic Shortcomings

In September 2022, Datos Insights (then Aite-Novarica Group) published a taxonomy for financial services CISOs and leaders to better view several subdomains related to identity in the market (Figure 1).

Figure 1: Datos Insights' 2022 Identity Taxonomy



The taxonomy was discussed with CISO members of Datos Insights' Cyber Executive Councils as well as leaders outside the councils. The taxonomy helped CISOs and other identity leaders understand the numerous, complex, interconnected subdomains of identity solutions while highlighting subdomains that warranted planning and budget activities for future investments. This view of identity subdomains also helped leaders reflect on where they had been investing within digital identity capability for the past few years.

Identity Investment Themes in 2023

In discussions with financial services CISOs in 2023, some through surveys with Datos Insights FI and Insurer Cyber Executive Council members, these leaders expressed attack surface management concerns related to IT estate complexity and sprawl and frustrations tied to the inability to retire tech debt tied to legacy identity stores. We observed CISOs and other leaders investing in digital identity in three primary ways:

- **User-centric MFA features:** Driven by the COVID-19 pandemic and an urgent need to support remote worker scenarios, most FIs deployed upgrades to authentication and identity systems in 2023. Some deployed older one-time-passcode (OTP) capabilities, but Datos Insights' research indicated phishing-resistant MFA was the top identity security investment across all FIs. Through a separate research effort with 100 North American and European FIs, Datos Insights found that 82% initiated phishing-resistant MFA deployments in 2023 to be completed in 2024.

- **Workforce identity platforms:** Enterprise-grade identity platforms were a strong investment for many FIs in 2023. Driven by the pandemic and unprecedented work-from-home dynamics, identity platform investments represented urgent CISO responses to enterprise remote access risk in 2023. Of 100 FIs surveyed across North America and Europe, 76% were evaluating workforce identity platforms in 2023, securing budget for deployment in 2024.

- **Identity governance and administration (IGA) and privileged access management (PAM) tools:** Of 100 FIs surveyed across North America and Europe, 80% were completing modernization projects for PAM, virtual private network (VPN) replacement, and insider cyberattacks in 2023. Driven by ongoing audit and regulatory compliance, many FIs were operating in year two or three of deploying their IGA tools. Of all components within the identity ecosystem, IGA held the highest degree of CISO frustration and "buyer's regret" due to the ongoing staff impact from never-ending projects, as well as heavy staff impact with manual tasks and policy reviews.

Common Challenges and Shortcomings

These investment tendencies leave shortcomings common to many FIs and insurers. With a focus largely on user-centric features, regulatory compliance, and security point solutions, financial services CISOs and their teams generally gave less attention to higher-order identity framework opportunities. Many of the problems these leaders faced were held in common:

- **IT estate sprawl and complexity:** Both added attack surface to the businesses, increasing cyber risk.
- **Limited data sharing and risk signaling between solutions:** Identity and security point solution integrations were limited to "adjacent" components without an overall ecosystem data view.
- **Siloed views of users:** Disjointed and incomplete user views were another byproduct of identity and security point solutions.

These common problems generally required more systemic, framework-style solution approaches. In a practical sense, years of investment priority focused on user-centric features, compliance, and last-mile defenses resulted in security and identity silos within the enterprise, creating new, more difficult challenges for CISOs.

Traditional Identity Has Contributed to Enterprise Complexity

While considerable progress has been made over the last three decades, much work remains for financial services digital enterprises. An honest assessment says cybersecurity remains complicated and operationally immature for CISOs. Complex IT estates are the institutional norm. Most CISOs would concede they face greater operational complexity than they did five years ago, and the prevailing trend is toward even greater complexity. This analyst believes that identity implemented poorly in the traditional IAM mindset has contributed to enterprise complexity for most CISOs. Through a strategic lens, traditional identity is poor, with low assurance. Largely siloed security solutions, such as IGA and PAM, do their best to operate with a kind of shadow (low confidence) of the user's identity, and they have done remarkably well at mitigating risk under these circumstances. The financial services industry has progressed forward.

Using a medical metaphor, this advisor views low-quality identity as the underlying problem, and largely siloed security tools as enterprise "coping mechanisms." IGA, PAM, and other important security tools deliver critical risk management functions, but they are more complicated and siloed than practitioners desire and masking the underlying problem—identity. Enterprise speed of delivery is severely constrained given these realities. In 2024, FIs and insurers must recognize that the proliferation of siloed security solutions is a symptom of underlying poor identity, which adds complexity, increases cyber risk, and slows the business. Can we imagine a more agile digital enterprise operating with fewer, better integrated, and more efficient security solutions? Modern identity structures hold the key to these business-critical outcomes.

Lack of Identity Progress in U.S. Public Sector—Headwind for Financial Services

The U.S. federal government has achieved modest progress toward strategic identity capabilities. CISA's strong urging of phishing-resistant MFA,[5] identity's strong position within NIST's Zero Trust Security Model,[6] identity's inclusion in the White House's executive order on cybersecurity,[7] and CISA's "more than a password" campaign[8] all required hard work and should be celebrated. But these accomplishments represent modest, early-stage milestones. As a recent example, key opportunities for citizens to operate with REAL-ID through mDLs are currently limited to face-to-face use cases under Department of Homeland Security (DHS) authority. In December 2023, leaders urged Congress to task NIST with developing standards for more impactful online use cases for mDLs to invigorate transitioning of citizens to digital forms of authoritative identity.[9] Digital identity progress in the U.S. public sector remains stuck, while other countries continue to proceed forward toward much more meaningful outcomes.

Despite the clear need and broad consensus, the U.S. public sector lacks a champion to drive how citizens operate with digital identity credentials. Transformational societal impact continues to stall in the U.S., hampering FIs and insurers in their support for more modern identity mechanisms. Conversely, great opportunity exists for public sector advancement of citizens using secure digital identity claims such as mDL. Stronger federal investment and tangible mDL progress would significantly influence citizens regarding this important transition to digital identity and provide a natural tailwind for financial services firms as they modernize identity for their workforce and customers.

---

5 "Implementing Phishing-Resistant MFA," CISA, accessed February 21, 2024.

6 "Zero Trust Maturity Model Version 2.0," CISA, April 2023, accessed February 21, 2024, https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

7 "Executive Order on Improving the Nation's Cybersecurity," The White House, May 12, 2021, accessed February 21, 2024, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

8 "More Than a Password: Protect Yourself From Malicious Hackers With Multifactor Authentication," CISA, June 2022, accessed February 21, 2024, https://www.cisa.gov/MFA.

9 "NIST Should Be Tasked With mDL Standards, Experts Tell Congressional Hearing," Mobile ID World, December 7, 2023, accessed February 21, 2024, https://mobileidworld.com/nist-should-be-tasked-with-mdl-standards-experts-tell-congressional-hearing/.

Elevating Identity Beyond IAM—A New Mindset for Financial Services

Financial services firms have considerable challenges in a difficult market. CISOs and other identity leaders within the organization need to focus on digital identity in base business terms, which, for some leaders, represents a major change from traditional IAM norms.

Elevating the Business Requires Elevating the Identity Mindset

Historically, identity relates to IAM, a well-known technical domain tied to risk and compliance. However, through the lens of business—and taking inventory of modern identity capabilities—the phrase "IAM" has become ill-suited to contain the means through which identity is needed to transform the business. As modern identity solutions have evolved considerably, CISOs and other identity leaders need to think very differently about the power of identity. Business enablement matters more than technical protocols. Table A highlights major aspects of this strategic mindset shift.

Table A: Elevating the Identity Mindset for the Business

Traditional: Identity as IT burden	New: Identity as a key business enabler
Identity is known as an unavoidable tech burden, in traditional IAM mindsets, with an information security focus on controlling and managing access.	Identity is designed as a cornerstone for the business, with goals beyond infosec to enable a more operationally mature enterprise.
Low identity assurance (confidence) leads to security point solutions and operational silos that slow the business.	High identity assurance enables the enterprise to streamline security solutions so the business can accelerate and achieve real digital transformation.
Identity data is inconsistent and redundant across the enterprise, compounding IT sprawl, complexity, and attack surfaces.	Identity data is centralized within the enterprise, delivering consistent, authoritative identity data to all enterprise services.
Identity enables point-in-time risk assessment and policy decisions, which can be manual, time-consuming, and of low quality.	Identity and security are designed for continuous risk assessment, with automation to reduce time and increase the security of common tasks.
Multivendor identity point solutions lack integration quality, cross-platform	Multipurpose identity platforms function as "ground zero" for delivering high resilience,

Traditional: Identity as IT burden	New: Identity as a key business enabler
instrumentation, automated risk mitigation, and (at times) accountability.	improved risk mitigation, and increased integration quality.
Traditional identity claims, such as passwords, operate as shared secrets that are no longer secret, leading to more than 80% of compromises annually.	Identity claims are elevated to phishing-resistant MFA, deployed to the workforce, partners, and customers, deprecating passwords and reducing cyber risk for the business.
Identity has become distinguished from authentication, but it often carries different meanings depending on context, vendor, and speaker.	Identity, authentication, and intent (new term) are distinct yet complementary concepts that facilitate the collaborative development of new, more robust solutions.

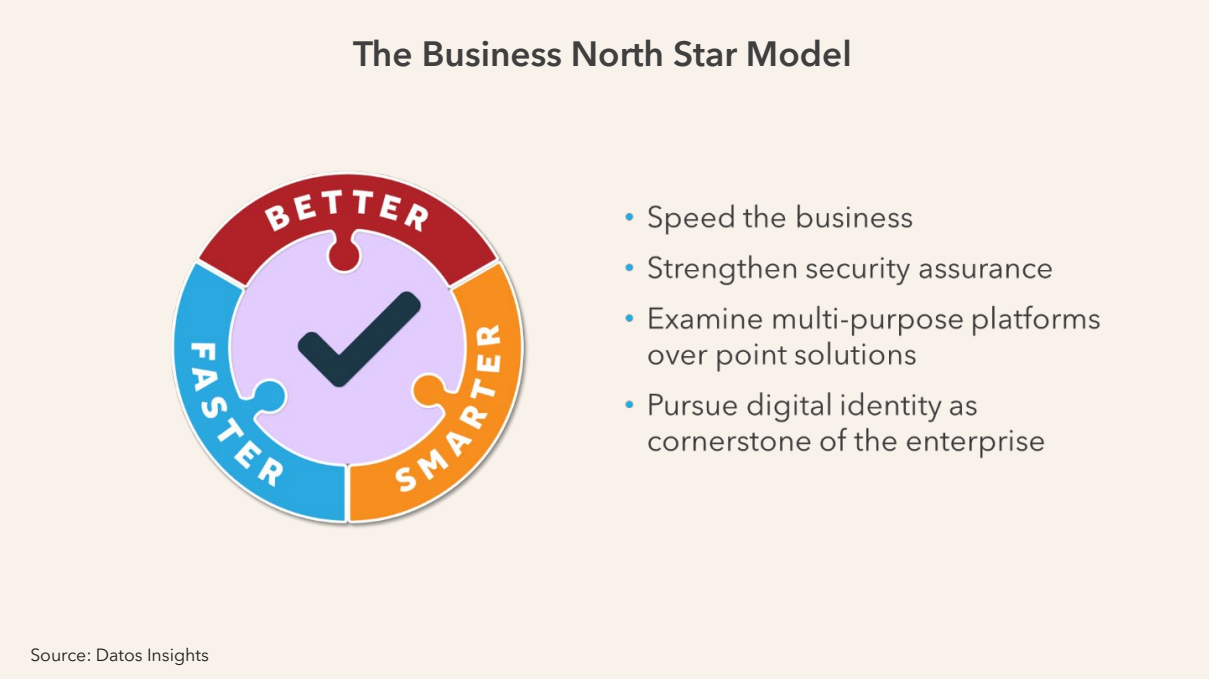
Source: Datos Insights

This identity mindset shift can be challenging for many, including seasoned identity and cybersecurity professionals. Bias toward historical IAM norms tends to be pervasive across organizations. Yet, even with difficulties noted, CISOs who can find needed domain expertise and build strong peer partnerships can transform their businesses through these identity-led pursuits. Strategic outcomes are becoming increasingly realistic through innovative solutions found in the market.

"North Star" for Identity—Enable More Operationally Mature and Secure Enterprise

With multitudes of priorities and security domains under their remit, CISOs have one of the most demanding executive roles within financial services. In frequent chaos and often conflicting priorities, what North Star can help guide CISO tactical and strategic decisions? A North Star must be difficult and durable, reflecting the customer a solution is intended to serve. As the customer for identity and cybersecurity is the business, Datos Insights recommends the Business North Star model (Figure 2).

Figure 2: Identity North Star—Enable More Operationally Mature and Secure Enterprise



Source: Datos Insights

In serving the digital enterprise, the delivery engine of the business, strategic identity solutions must make the operational maturity and security of the enterprise its ultimate pursuit. Business agility, operational simplicity, more cohesive and intelligent functionality, and more predictable and measurable cyber risk are among these top objectives. As any seasoned professional knows, these simply stated business concepts are nontrivial to reach. They may be impossible to achieve without digital identity stretching beyond traditional IAM norms to new kinds of strategic capability. Simplicity, as Steve Jobs famously shared, "is the ultimate sophistication."[10] As this lesson has been retold thousands of times since, simplicity comes by *conquering* complexity rather than by avoiding it. Financial services operate with significant IT complexity, of which security and identity are critical components. CISOs and other identity leaders must look for solutions not entirely focused on user features or compliance mandates. Rather, they must seek identity framework solutions that conquer underlying security complexity so that overall enterprise maturity can be achieved.

[10] Walter Isaacson, "How Steve Jobs' Love of Simplicity Fueled a Design Revolution," Smithsonian Magazine, September 2012, accessed February 21, 2024, https://www.smithsonianmag.com/arts-culture/how-steve-jobs-love-of-simplicity-fueled-a-design-revolution-23868877/.

Strategic Identity Capability for FIs and Insurers

For financial services firms looking to transform their business agility and security assurance, modern identity framework solutions hold the key. Many CISOs and identity leaders need guidance on how to approach core channels within their institutions and the kinds of strategic solutions to seek.

Workforce, Partner, and Customer Channels

FIs and insurers have historically operated in three separate "identity islands" within the organization. Identity solutions serving the workforce (aka workforce IAM, enterprise IAM) tend to be isolated from solutions serving customers (often referred to as CIAM solutions). These islands within the business are largely isolated from one another, with distinct solutions, people, processes, and key performance indicators. A third part of the business involves business partners (aka third parties, vendors, suppliers), typically operating on their own island. Datos Insights recommends that CISOs view identity strategy and ownership across these three channels of business in the following manner (Table B).

Table B: Recommendations for Primary Business Channels

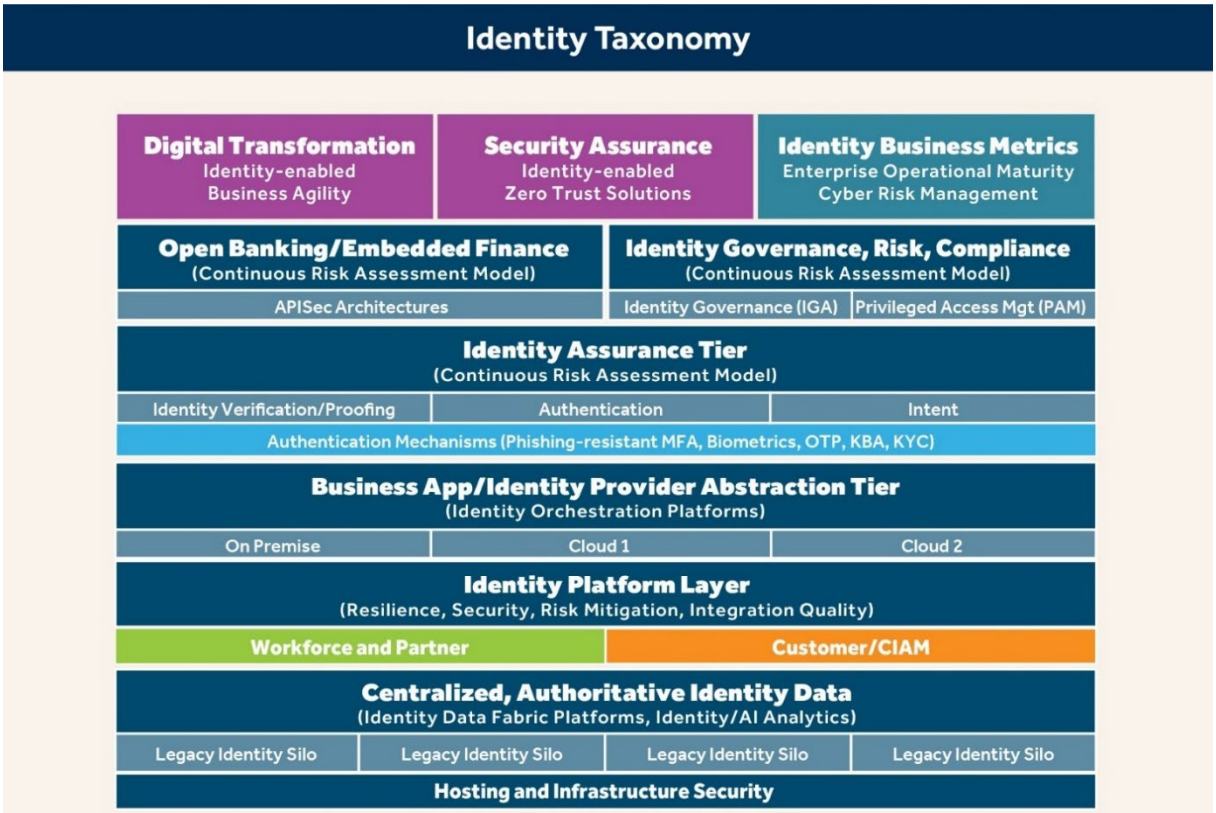
Datos Insights recommendations	Additional comments
Consolidate identity for workforce and partner channels under the CISO. Identity budget, strategy, and operational ownership are well suited to be brought together.	Business drivers are similar and can be reconciled by CISOs. For most institutions, partner identity urgently needs executive attention in response to heightened third-party and supply chain risks.
Keep the CIAM channel separate. Business drivers for consumer services are distinct and call for different identity solutions.	CIAM holds distinct business drivers and operational realities from workforce IAM. Some firms may choose to consolidate their CIAM budget under CISOs. Datos Insights' research indicates that CISOs are emerging as budget-owners for CIAM within financial services.
Strategic, cross-cutting identity capability can lift value for each channel.	An evolution of identity mindset, plus investment in strategic identity framework, can elevate each channel, even as deployed solutions may vary.

Source: Datos Insights

Recommended Strategic Identity Capabilities

Strategic identity capability can be difficult for CISOs and identity leaders to pinpoint—cutting through the vast number of identity solutions in the market, as well as the noise within institutions, is not easy. However, by using the North Star of business enablement and creating a more operationally mature and secure enterprise, a distinct capability set comes into view. Datos Insights' updated identity taxonomy is shown in Figure 3.

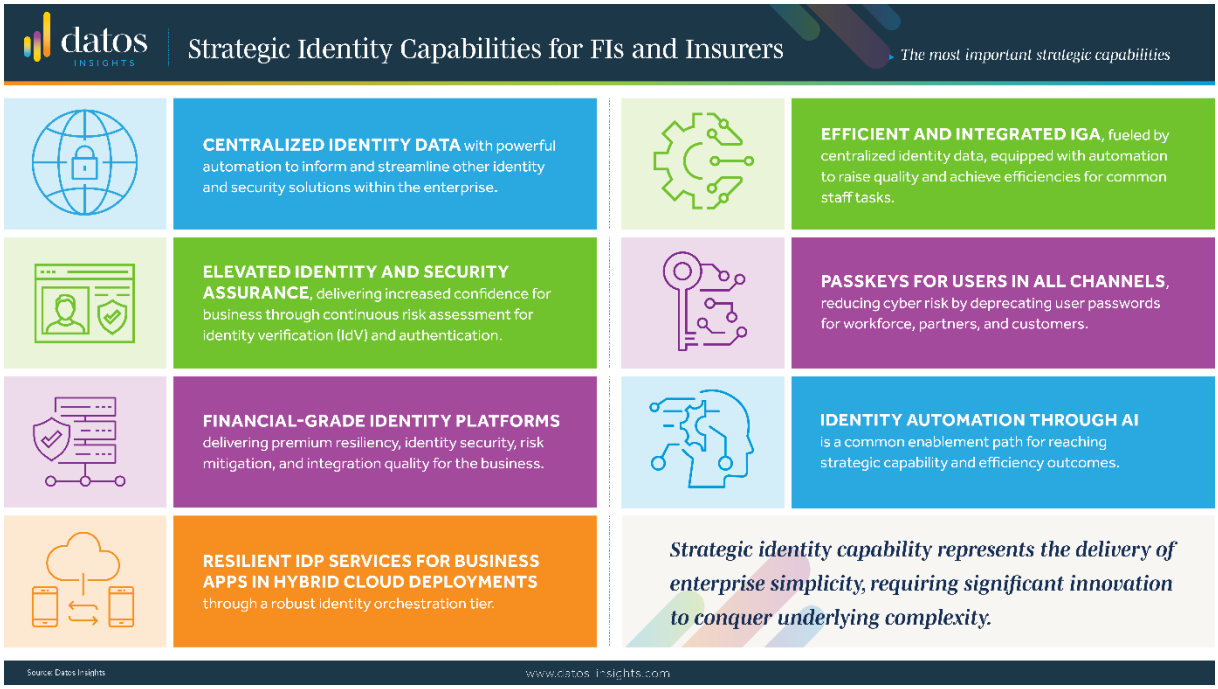
Figure 3: Updated Taxonomy for Transformative Identity



Source: Datos Insights, February 2024

The updated taxonomy was informed through analysis and discussions over the past year and by deeper consideration of what FIs, insurers, and other financial services firms need most from digital identity to ignite their businesses. Other industries need much the same. Improvements bring greater emphasis to abstraction layers (tiers) in which underlying complexity can be conquered and delivered in more simplified and empowering manners. Figure 4 summarizes the most important strategic capabilities.

Figure 4: Strategic Identity Capabilities for FIs and Insurers



The strategic capabilities included above are not listed in priority order. In most situations, achieving strategic identity capability represents the delivery of *simplicity* for the enterprise, requiring significant innovation to conquer underlying complexity.

Centralized Identity Data to Power the Enterprise

For many FIs and insurers, identity is distributed across the enterprise. Held by numerous lightweight direct access protocol (LDAP) identity stores in legacy containers, user identity is distributed, often redundant, and disjointed from an enterprise perspective. Financial services firms have operated this way for years, coping through fragile technical integrations between business applications and legacy identity stores. Few have the expertise or tenacity to deprecate this tech debt. This advisor has heard firsthand comments such as "we're getting by" or "the roof is not leaking too badly," usually followed by some general aspiration goal to retire identity tech debt "someday." A decade passes, mergers and acquisitions occur, and identity tech debt has become part of massive IT sprawl. Enterprise data quality for services tied to identity suffers.

A centralized identity data fabric layer is the first framework component highlighted in this report. In a data-driven world, centralized, normalized identity data is paramount to business success. For a strategic enterprise, identity data must function as an institution's cornerstone asset, reused in a common manner by all applications. Identity data in a single

format should inform (in the Just-in-Time inventory management model) the security functions rendered within the enterprise. The identity data fabric layer abstracts details of the identity data store (tech debt) and is called by consuming applications (e.g., identity platforms, business applications). Short-term gains from an identity data fabric layer are important. Identity platforms and business applications begin to consume identity data in the same way. The intelligence available through this single, inline abstraction layer becomes powerful for the business. This fundamental construct helps CISOs modernize and simplify the IT estate and retire identity tech debt.

The medium- and long-term business impacts are profound. Once a centralized source of identity truth exists within an enterprise, automation (usually through AI) can help the business achieve businesswide identity visibility. Auto-discovery of unmanaged identity or patterns of access within the enterprise has both security and operational benefits. Enterprises gain a powerful, strategic foothold to understand base user behaviors and anomalous patterns. As CISOs and identity leaders gain confidence in centralized source-of-truth identity data, opportunities to inform identity platforms, IGA tools, PAM tools, and security operations (SecOps) can emerge to drive more holistic views of user data, better security control decisions, and enable tooling efficiencies. As FIs and insurers operate in a data-driven world, they should seek providers of centralized and normalized identity data to better speed and secure their enterprise.

Elevated Identity and Security Assurance Delivers Increased Confidence to Businesses

Identity assurance and security assurance are intended to convey degrees of *confidence* delivered to businesses from a specific method or set of solutions, specifically that a user is who that person claims to be, both for initial and revisiting use cases. Assurance is not a new security concept. It was rigorously documented by NIST in 2017 and is well understood by seasoned identity and cybersecurity professionals.[11] In practice, within financial services, assurance levels specified by NIST function as guides toward risk-based identity verification (IdV) and authentication services. These solutions are delivered distinctly for the businesses' workforce (aka enterprise) and customer channels (aka CIAM). Within each channel, IdV and authentication services tend to operate as security silos with limited integration and data sharing.

[11] Paul A. Grassi, Michael E. Garcia, and James L. Fenton, "NIST Special Publication 800-63-3, Digital Identity Guidelines," NIST, June 2017, accessed February 5, 2024, https://pages.nist.gov/800-63-3/sp800-63-3.html.

It is important to remind CISOs and identity leaders that current specifications and solutions for identity and authentication assurance are *point-in-time* in nature.[12] That is, they focus on identity and security risk assessment and confidence at *one* moment. Point-in-time risk assessment has served as a bedrock for financial services and other industries for years. Still, its effectiveness has begun to wane through the past decade of data breaches and more sophisticated cyberattacks. Point-in-time risk assessment tools are unable to detect factors that change between assessment points (such as a user falling prey to a phishing attack) or capture ebbs and flows in how a user acts against services over longer periods. CISOs and other financial services leaders need identity and security assurance to be reimagined by products and services that deliver *continuous* risk assessment to create greater confidence (assurance) value for the business.[13]

Continuous risk assessment for identity and security assurance would produce transformative impacts for CISOs and the enterprises they are charged to secure. Three critical benefits can be enabled:

- Continuous risk assessment models should result in more holistic views of users and risk instead of limited point-in-time views. These models would enable the security ecosystem of currently siloed tools (e.g., IGA, PAM, MFA, governance) to become more intelligent and cohesive, be better integrated within the identity security ecosystem, and be more effective for the enterprise.

- A more intelligent and effective enterprise enables a business to move at greater speed and agility. Solutions that operate in continuous risk mode should improve the value cost basis for an enterprise, delivering identity and security confidence to the business.

- Deployed properly, continuous risk assessment should tear down historical silos between IdV and authentication and improve efficiencies for the business. Employees operate with enterprise services over a career of different roles and responsibilities. Consumers operate with customer services over a lifetime of events and needs in different seasons of life.

---

[12] Current identity assurance specifications also assume physical presence as a means to increased assurance.

[13] The need to drive to continuous risk assessment models is a theme for other security domains in the market. See Datos Insights' report Third-Party Risk Management for Financial Services: The Call for Greater Operational Maturity, June 2023.

Financial-Grade Identity Platforms: Premium Resilience, Risk Mitigation, and Integration Quality

The notion of a centralized identity platform makes common sense to most CISOs and identity leaders. Historically, phrases such as "IAM platform" and "IAM tool" were more commonly used, but recently, the term "identity platform" has risen in prominence. In 2021, Okta defined an identity platform as the following:

> "a modern solution for managing the identities of users and devices in a centralized fashion. It enables organizations to securely authorize workforce and customer users to access their ecosystem using access management tools, programmable components, integrations, and platform services."[14]

This definition may seem long-winded, but this analyst finds it well-stated, touching on key modern aspects and dimensions of value. Datos Insights' research indicates that most FIs pursue identity platforms through a single vendor, some through an integrated combination of vendors (which, collectively, they describe as their "platform"), or in the case of CIAM, leverage the identity platform offered by their digital banking provider.

Elevated Identity Platform Quality—Premium Resiliency Characteristics

The business criticality of the centralized identity platform has risen considerably. FIs suffer enormous financial damage whenever their CIAM platform becomes inoperable for any length of time. Outages for workforce and partner platforms produce significant damage to the business. Viewed against modern business expectations and those in the future, the *resilience* (availability) of identity platforms is the key value deficit. When multiple vendors are involved, the lowest component availability drives overall platform availability.

FIs and insurers need *financial-grade* identity platforms. This means delivering premium levels of resiliency and availability options for FIs and insurers that require it as a foundation for business success. This advisor translates premium levels of availability to "zero downtime" identity platforms or closely approximating these standards. This lofty operational target will not manifest overnight, and it is so demanding that only top identity providers in the market may pursue these goals. Of course, not all customers require this degree of operational quality. However, this is a strategic capability some financial services firms need now. Many more will require it in the future.

---

[14] Arun Singh, "What Is an Identity Platform?," Okta, July 7, 2021, accessed February 12, 2024, https://www.okta.com/blog/2021/07/what-is-an-identity-platform/.

Elevated Identity Platform Quality—Premium Risk Mitigation Capability

Noteworthy data breaches have occurred over the past few years wherein attackers have ultimately beaten an identity platform or the company providing the identity platform. In many contemporary incidents, the blast radius of the breach (number of customers or users impacted) was unacceptably large.

FIs and insurers need financial-grade identity platforms for attacks that successfully reach the platform. Thus, the strategic platform must deliver a new premium-style risk detection and mitigation capability with new kinds of operational controls that detect attacks and significantly improve risk mitigation when a breach occurs. Standard risk signaling channels are key to making this operational for multi-vendor deployments. Minimizing the blast radius through automated capability, straightforward configuration, or simple manual operation is what many financial services firms need. As with premium platform resiliency, premium risk mitigation capability is a high bar. Only some providers may aspire to it and not all customers will require it. Still, for many FIs and insurers, premium platform risk mitigation functionality is highly sought after.

Elevated Identity Platform Quality—Premium Security Integration

In other incidents, analysis showed that the deployment of some kind of MFA would have reduced or in some cases prevented business damage. This was especially frustrating when providers had MFA capability at the ready, but the customer did not implement MFA for various reasons. In the aftermath, some pointed fingers instead of solving problems.

FIs and insurers need financial-grade identity platforms. This means a new, premium-level integration service with MFA and other protections implemented as the base. This advisor recommends phishing-resistant MFA as the base and a formal certification process to ensure it. But the essential recommendation is MFA implemented as part of the base for this new service tier—not left to the customer or the integrating partner to decide. In time, this model may include other base defenses. Lower (nonpremium) service levels should remain for customers with lower business demands who accept higher associated risks. A premium service with MFA as the base is a high perch only some identity platform providers may aspire to. But it is what many FIs, insurers, and other customers need.

Resilient Identity Integrations for Business Applications in Hybrid Cloud Deployments

The proliferation of cloud-computing environments has transformed how FIs and insurers view and operate their digital enterprise. Many FIs operate in hybrid cloud deployments, with an on-premises enterprise deployment and multiple cloud footprints. Some cloud deployments are the direct choice of the FI, while others are the result of an FI's partners and third parties that deliver using Software-as-a-Service (SaaS) models. Datos Insights research indicates that insurers often operate through a single public cloud vendor plus cloud deployments from third parties. An institution's cloud deployments have added complexity for the CISO and other operational leaders. Digital identity is one of the more challenging aspects of hybrid cloud deployments. Business applications deployed within cloud deployments must integrate to identity provider (IdP) services deployed in different cloud environments. In the traditional model, business applications must be configured to understand the details of IdP services, a pattern that scales poorly, is expensive to maintain, adds operational risk for IdP failure scenarios, and layers on further complexity to the enterprise. Vendor IdP selections tend to become locked in, with migrations to new IdPs carrying high technical and operational risk to the business.

FIs and insurers need strategic IdP integrations for their business applications within hybrid cloud deployments, which look like more abstracted IdP integration models. In the pursuit of operational simplicity, CISOs and technical leaders need an abstraction tier through which business applications can access IdP services in a manner like accessing utility services, such as domain network services (DNS), without being coupled to IdP cloud hosting details. "Identity orchestration" is the term used to describe this kind of capability in the market.

Using an identity orchestration platform, a business can operate across its hybrid cloud environment without its business applications knowing or managing identity details. This operational decoupling of IdP services can simplify the IT estate and create tremendous operational value for the enterprise. For some businesses, this capability can serve as the lynchpin for moving more business applications to the cloud while maintaining current IdPs behind the abstraction tier. For others, this decoupling capability can enable the business to move to a new identity vendor, removing lock-in from an identity vendor that is not performing well. The business can become more agile with its applications and reduce time to revenue. IdP modernization efforts can be accomplished behind the scenes without business applications recoding to accommodate changes. And perhaps most importantly, the business can improve IdP resiliency considerably. Designed correctly, an

identity orchestration platform should detect a failed or failing IdP and quickly route to an alternative, available IdP service. This kind of strategic identity capability has a profound impact on the enterprise and how it can operate. In a cybersecurity market where much attention has been brought to the need to "shift left" into secure design, an industry expert recently commented that identity orchestration implemented well represents a strategic "shift right" for better operationalizing enterprise-grade identity. This analyst wholeheartedly agrees!

Identity Governance Reimagined

Operating within the traditional IAM mindset, IGA has served the market well for years. IGA is a critical function for a financial services firm, anchoring the management and audit for access rights of users to services, conducting regular policy reviews, and demonstrating compliance for access management.

Traditional IGA solutions have become a growing pain point for many FIs and insurers, tending to operate as silos within CISOs' ecosystems of security solutions. Common repeated tasks such as policy reviews are heavily manual, highly impacting CISO teams and managers given responsibility for conducting periodic access reviews for their teams. Within the Datos Insights FI Cyber Executive Council, in 2023, one CISO expressed that IGA solutions have the highest degree of buyer's remorse, with the FI growing weary of manual tasks and never-ending IGA projects. Other CISOs quickly concurred. The manual nature of traditional IGA also tends to drive lower security outcomes for the business. The IGA pain expressed by CISOs does not appear tied to a specific vendor product but instead presents as an overall operational theme across IGA products. With all the meaningful value IGA brings, this analyst believes most traditional IGA products have simply become inefficient for CISOs and their businesses.

IGA reimagined for a business starts with IGA becoming less siloed and more integrated within the security ecosystem. IGA can still be distinct and special but not siloed. IGA reimagined must also elevate to higher quality by taking dependency on centralized, authoritative user identity within the enterprise instead of finding and governing access to identity it knows about. IGA reimagined means driving common tasks to become more automated and more efficient for CISO staff. In other words, IGA solutions need to become more "lean and mean" to drive staff efficiencies. By taking dependency on enterprisewide centralized user identity and driving automation through AI, heavy manual tasks can become displaced with intuitive, streamlined tasks so that CISO staff and people managers complete these tasks in less time and with greater security. From the perspective of an FI

or insurer security organization, IGA reimagined includes a mindset evolution from IGA as a never-ending project to an ongoing practice the CISO optimizes within the enterprise.

Passkeys and Eliminating Passwords

This report cautions against an exclusive focus on user-centric identity features so CISOs and other identity leaders can examine strategic identity capabilities that can truly transform their businesses. However, one user-centric feature bears strategic consideration for financial services firms: passkeys and the critical charge to deprecate passwords. Passwords and other shared secrets are compromised due to previous and ongoing data breaches combined with phishing attacks, which are increasingly effective and empowered by adversarial AI. Only the adversarial AI dimension is new news.

Cyber risk problems tied to user passwords are well known. CISA strongly urged phishing-resistant MFA in October 2022.[15] Datos Insights advised FIs and insurers of the need to migrate to phishing-resistant MFA in September 2022. A close examination of passkeys,[16] the FIDO2 standard-based phishing-resistant MFA solution, show that both usability and security are improved for passkeys as compared to user passwords. The traditional balance between user experience and security is reimagined through passkeys. Still, progress toward phishing-resistant MFA within financial services remains low. Successful attacks rooted in easily beating passwords remain high. In January 2024, the Better Identity Coalition continued the drumbeat, sharing that over 80% of 2023 data breaches were related to stolen, weak, or reused passwords.[17]

Given all the headlines and advancements in the market, why do passwords persist within financial services? This analyst suggests six primary reasons:

- **Too many terms:** Some market vendors call this capability passwordless MFA. Others call it phishing-resistant MFA (the phrase this analyst tends to use in discussions with seasoned industry veterans). Still, others refer to it as certificate-based authentication (CBA). Finally, others call it a passkey. No one is incorrect, per se. Vendors have every right to name a functionality how they wish and to highlight value distinctions through their brand label. But from a landscape perspective, these many names add complexity and confusion for CISOs or other financial services buyers, a persona that is

[15] "Implementing Phishing-Resistant MFA," CISA, accessed February 22, 2024.

[16] For more detailed understanding of passkeys and the FIDO Alliance, see https://fidoalliance.org/.

[17] "Better Identity Coalition: Better Identity at Five Years: An Updated Blueprint for Policymakers," January 2024, accessed February 28, 2024, https://static1.squarespace.com/static/5a7b7a8490bade8a77c07789/t/65b00995dd1af8633cbce40c/1706035608068/Better_Identity_Coalition24.pdf.

increasingly business-centered. All things considered, this analyst recommends the market align around the term "passkeys" for this functionality and describe distinctions from this basis. This step would help business sponsors better understand this important capability, removing confusion and friction in the evaluation and buying process.

- **Usability concerns:** A legitimate concern for financial services firms was how users would leverage passkey workflows. But through the excellent work of the FIDO User Experience Working Group, user journeys associated with passkeys are now demonstrated, documented, and well understood.[18] Opt-in models offering passkeys at specific points in consumer journeys have emerged as a best practice.

- **Lack of operational comfort:** No one likes passwords (other than cyber criminals). However, decades of use have fostered robust operational processes within organizations to support user passwords. These processes are entrenched so deeply within some businesses that support teams cannot imagine supporting users without passwords. Operational comfort with passwords may be too strong a phrase, but operational discomfort certainly exists for passkeys within many FIs and insurer support organizations.

- **Lack of a societal drivers in the U.S.:** The U.S. public sector continues to lack a champion and investment to encourage citizens to embrace digital forms of identity such as mDLs for online use cases. Without this citizen and societal transition, FIs and insurers face additional headwinds in deploying modern identity features such as passkeys, and deprecating passwords. Passkeys should be envisioned as having societal impact beyond financial services and other industries.

- **Fixation on consumer use cases:** There has been much focus on passkeys for consumer services at FIs, insurers, and other financial services firms. In addition to usability and security benefits, FIs have hard costs associated with password resets, and efficiency gains to be realized through passkeys. But many FIs have found alternative means to gain efficiencies, and other headwinds for passkeys have resulted in slow or stalled consumer campaigns. Through partnering with their identity vendors, more creative institutions have introduced passkeys first into their digital workforce. The workforce offers many advantages for passkey introduction, including the ability to dictate adoption, smaller user populations, more clarity in supportability, and lower business risk compared to introducing this functionality to consumers. Passkeys for consumer-

[18] "Technical Working Groups," FIDO Alliance, accessed February 22, 2024, https://fidoalliance.org/members/working-groups/.

based services remain an important strategic consideration for financial services. But an approach that considers passkeys a means to modernize the workforce, increase MFA resiliency in the face of phishing attacks, reduce enterprise cyber risk, and build organizational "muscle memory" around passwordless support is a wise approach that many FIs and insurers should seriously consider. Workforce deployment of passkeys can be how an institution prepares for introducing passkeys to its consumer base.

- **Some reticence to spend:** This may not exist at every financial services firm, but this analyst has observed that some firms are reluctant to invest in passkey capability. CISOs have a large remit. Add a challenging economy, and of course not everything the CISO desires gets funded. But all this said, CISOs and other leaders who truly desire to transform and reduce cyber risk for their businesses are strongly encouraged to make the business case and win the budget needed to introduce passkeys in some part of their business. There are many FIDO-certified passkey products available in the market. The time to act is now.

Intersection of AI and Strategic Identity

One can hardly have a cybersecurity discussion without AI (broadly), generative AI (more specifically), and cyber risk being addressed. Market security vendors within every domain are investing in AI-based value improvements and marketing advancements to clients and prospects.

As this report (and this analyst) assert the thesis that strategic digital identity is uniquely positioned to transform the business, an important recommendation concerns the intersection of AI and strategic identity. Most of the identity capabilities presented in this report *assume* the use of AI to achieve strategic value outcomes for FIs and insurers. Like identity, AI is a transformational force for CISOs. As *applied* to identity, AI can have a profound multiplier effect on how identity products can enable value for enterprises. AI is central to automating identity data discovery, automating risk mitigation methods, and a host of other premier value characteristics for CISOs and other executives.

Capabilities in the Market—The Identity-Enabled Future Is Now

Strategic identity solutions have become more than theoretical concepts and aspirations. Product capabilities have recently become available in the market that deliver some of the key aspects contained in this report. In 2024, CISOs and identity leaders at FIs and insurers should investigate these offerings, consider deployment options, and gain investment support for these kinds of strategic investments.

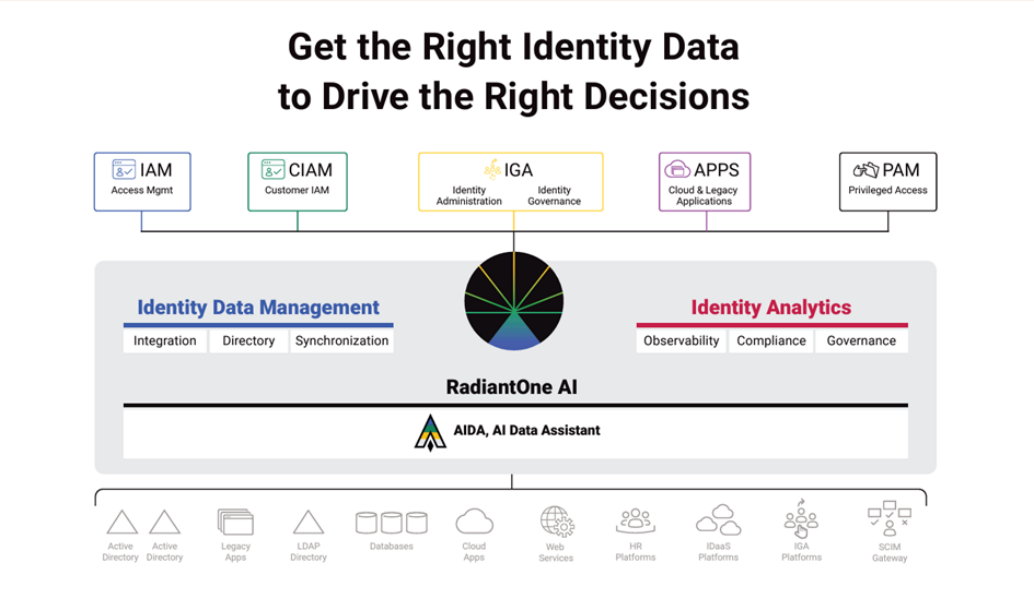
The following four providers are not intended to be a comprehensive market landscape. However, these four providers are a distinguished shortlist of visionary companies with high technical competencies ripe for transforming financial services through strategic identity capabilities. Continuous risk assessment is a common theme.

Radiant Logic RadiantOne Identity Data Platform

RadiantOne is an identity data management and analytics platform. Similar to an Informatica for identity, Radiant Logic enables organizations to harness identity data with advanced analytics to drive better business outcomes, improve security and compliance posture, increase speed-to-market, and more.

Radiant Logic's heritage is in virtual directories. It specializes in applying virtualization technologies to complex identity environments, so it becomes a singular, on-demand resource for the organization. With customers across Fortune 500 companies, Radiant Logic is built to simplify the management of the most highly regulated identity environments. Its recent acquisition of Brainwave GRC brings advanced analytics into the platform, allowing customers to achieve greater visibility and apply governance to their identity data (Figure 5).

Figure 5: Radiant Logic Identity Data Fabric



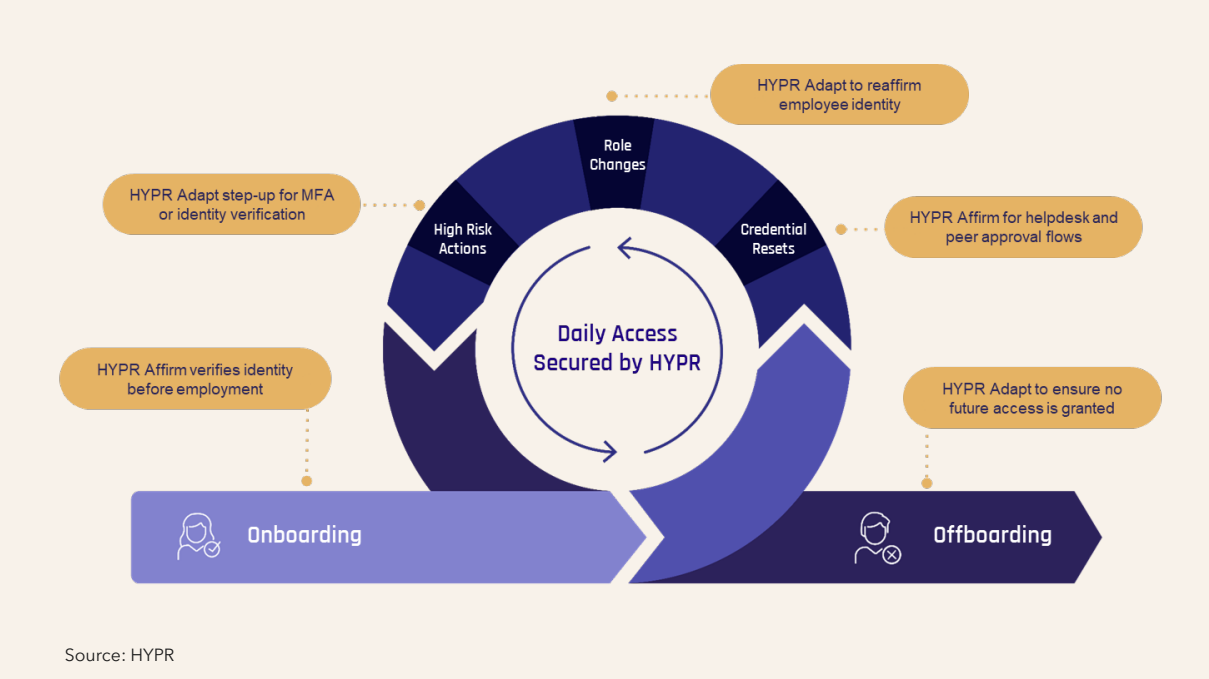
Source: Radiant Logic

Earlier this year, Radiant Logic announced RadiantOne AI, its data-lake-powered AI engine, and AIDA, its generative AI data assistant. These tools are designed to leverage identity data to understand and mitigate risk by taking advantage of the substantial enterprise data set that Radiant Logic can access. With RadiantOne's advanced data and relationship model, AIDA can see into every layer of the access chain to find and alert reviewers to any misallocated rights, which can then be automatically remediated under reviewer control. The first use case will be around streamlining user access reviews, which promises to bring AI-driven automation and operational efficiency to what is traditionally a very tedious manual process.

HYPR Identity Assurance Platform

HYPR is a leading provider of phishing-resistant MFA and identity risk mitigation for workforce and customer channels of business. HYPR's announcement of its HYPR Affirm identity verification solution in October 2023 builds upon previous capabilities and positions HYPR as an identity security disruptor with strategic value for financial services and other industries. At its core, HPYR Affirm centers on identity assurance and ushers this company into truly transformative identity security capability (Figure 6).

Figure 6: HYPR Brings Assurance to the Identity Life Cycle



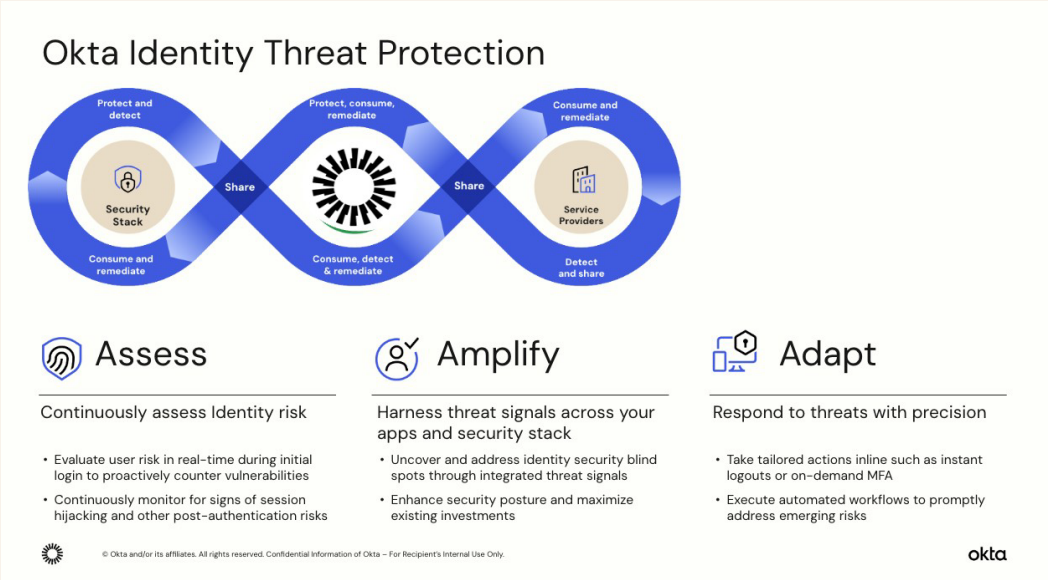
Source: HYPR

The integrated HYPR Identity Assurance platform maps to the market needs for passkeys and elevated identity and security assurance, which delivers increased confidence to the business. With an independently validated return on investment (ROI) of 324%, HYPR's solutions secure some of the most complex and demanding organizations, including two of the four largest U.S. banks, manufacturers, and leading critical infrastructure companies. Operating in the continuous risk assessment model, HYPR asserts that identity assurance requires knowing users are who they say they are, all the time.

Okta Identity Threat Protection

Okta is a global market leader for identity, with its flagship product in its identity security stack being Identity Threat Protection (ITP) with Okta AI. Okta developed ITP with Okta AI to reinvent identity security for the cloud-first era it helped usher in. Going beyond outdated access models, ITP is a continuous identity threat assessment and response platform that incorporates post-authentication protection enhancements using natively developed detections as well as third-party signals to reevaluate access and recover security posture for sessions and identities. ITP combines with other identity security offerings in its stack, viz.: ThreatInsight, Network Zones, Adaptive MFA, and Behaviors, to offer a zero trust, defense-in-depth identity security solution with core identity threat detection and response functionality (Figure 7).

Figure 7: Okta Continuous Risk Assessment—ITP



Source: Okta

There are three major capabilities where ITP delivers differentiating value for businesses:

- ITP's Risk Engine delivers Okta AI through a cohort of detections in ITP to mitigate and remediate session hijacking, brute force and other such tactics, techniques and procedures (TTPs) used by threat actors today. Detections for TTPs such as session hijacking can be mitigated and remediated in-line, through MFA, thereby preventing token issuance to a threat actor.

- ITP's signal sharing platform delivers OpenID's shared signals framework (SSF) to the broader vendor partner community. This allows customers to integrate their best-of-breed software, systems, and security providers with Okta so that they can exchange signals. The resulting pub-sub model of security information exchange mitigates security silos and enables holistic security protections across all threat surfaces for an organization. The SSF framework leverages continuous access evaluation protocol (CAEP), and Okta has partnered with some of the top security event providers, most notably, Palo Alto Networks, ZScaler, Jamf, and SGNL (10 officially qualifying as SSF security event providers, joining the existing list of OV security partners Crowdstrike and Windows Defender, with close to 30 more being added) to extend the capabilities of the Okta Risk Engine to reduce standing privileges and fully embrace a true zero trust model.

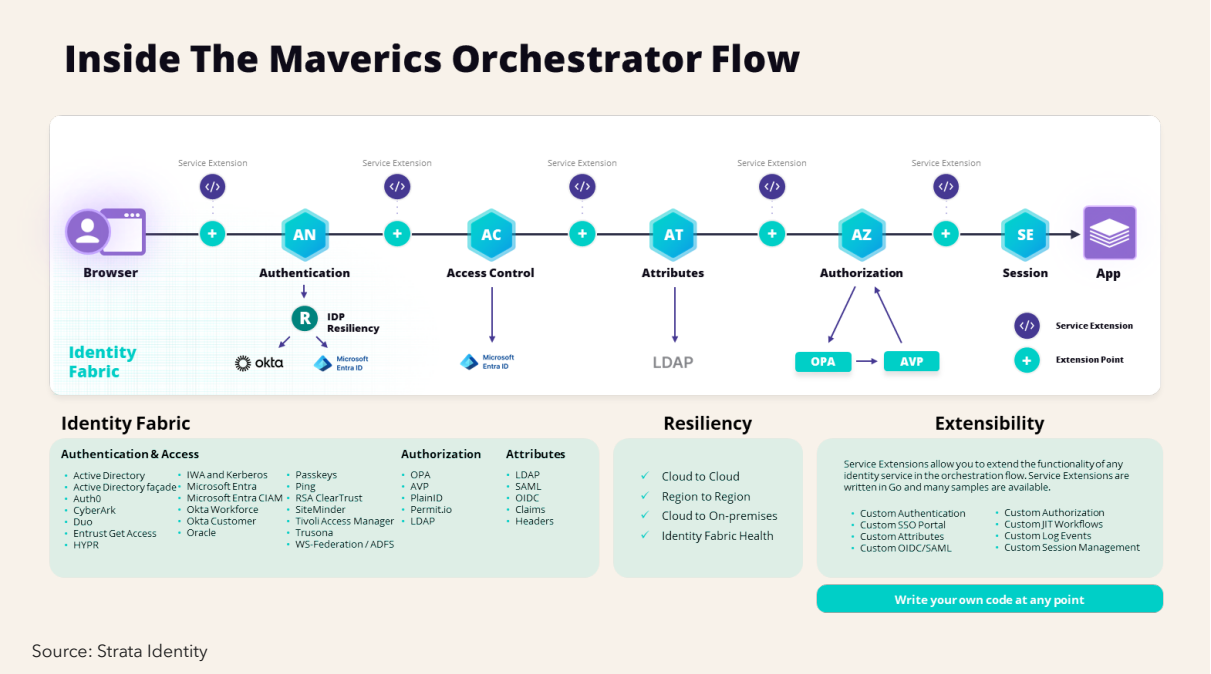
- ITP enables customers to establish unique access revocation capabilities within their organizations through universal logout, configurable within policy and API, to deliver a powerful containment and mitigation of the assessed threat/attack. Additionally, a customer can achieve more nuanced business process outcomes in incident response, orchestrated extensibly through workflows (e.g., quarantining a device, escalating identity assurance requirements on a user or placing them into a group, enforcing automated restrictions on data access, generating an incident ticket in queue for triage).

All this value can be monitored within intuitive, live views, and insights through dashboard widgets and reports on the identity security landscape of the organization.

Strata Identity Maverics

Strata Identity is the leader in identity orchestration for multi-cloud and hybrid cloud environments. The orchestration recipe-powered Maverics platform enables organizations to integrate and control incompatible identity systems with an identity fabric that does not change the user experience or require rewriting apps. By decoupling applications from identity, Maverics makes it possible to implement modern authentication, such as passwordless, and enforce consistent access policies without refactoring apps (Figure 8).

Figure 8: Strata Identity Maverics—Continuous IdP Abstraction Layer



Source: Strata Identity

Maverics also provides identity resilience in multi-cloud environments that ensures continuous access to applications even when a primary IdP is offline. The company's founders created the identity query language (IDQL) standard and Hexa open-source software for multi-cloud policy orchestration and are co-authors of the security assertion markup language (SAML) standard for federated single sign-on.

Identity Maturity Metrics for Financial Services

The elevation of identity mindset called for in this report includes recommendations for new operational business metrics. Datos Insights recommends the following strategic metrics for financial services.

Identity Security as Enterprise Maturity Metric

The evolving operational maturity of an FI or insurer's digital enterprise is a strategic, multiyear pursuit involving CISOs, CTOs, chief risk officers, and others. From several perspectives, strategic digital identity capability is central to this pursuit. Low operational maturity for the enterprise reflects increased cyber risk and business agility challenges and correlates to low identity assurance, lack of strategic identity investment, security point solutions, and significant identity tech debt. Low enterprise operational maturity broadly corresponds to CISA's call to "defend now." In comparison, high enterprise maturity represents lower corporate cyber risk and increased business transformation and agility, connecting to greater identity assurance (business confidence), strategic identity investment, more cohesive security platforms, and less identity tech debt. High enterprise security aligns with CISA's call to "secure tomorrow."

CISOs and chief risk officers at financial services firms need a business operational metric to convey to their boards that their enterprise maturity is tied to digital identity. This metric is intended to quantify both progress and deficits and help executives prioritize investment strategies for digital identity. This operational metric would also help considerably in mergers and acquisition scenarios, providing a potential acquiring party a better means to assess underlying enterprise complexity and identity maturity. Important to note: This enterprise maturity metric is envisioned as a sensitive business metric. It is not envisioned as a kind of publicly available Fitch Rating (disclosure of which would benefit cyber criminals). Rather, financial services firms would only share an enterprise maturity metric tied to identity security within a highly protected business relationship or inquiry. Standards bodies, such as NIST, working in collaboration with identity experts, are best positioned to create this operational metric.

Identity Security as Cyber Risk Management Metric

Cyber underwriting for financial services is in significant upheaval. At a January 2024 event hosted by the Massachusetts Institute of Technology Internet Policy Initiative, the Federal Reserve Board of Governors, and the Federal Reserve Bank of Richmond, the topic of cyber underwriting for financial services cyber risk was examined and discussed by industry leaders, policymakers, and researchers.[19] As leaders shared much progress to be celebrated, the formidable challenges ahead were recognized by all. As one bank chief risk officer shared with chagrin, "My new cyber underwriting policy costs more and covers less." Most in the room nodded.

Policy underwriters are accustomed to mature models that support risk probabilities within actuary disciplines. For financial services cyber risk underwriting, needed models are either in a nascent phase (view of some) or early phase (view of others) but generally lack *causative* data for models. A seasoned underwriter expert at the event shared his team's practical use of *correlative* data to generate meaningful policy at current model maturity.

At this stage, FI cyber underwriting needs additional correlative metrics. A metric for identity security maturity is recommended for inclusion. As the maturity of digital identity reflects the operational maturity of the enterprise, this analyst hypothesizes that it also correlates well to FI cyber risk. As a correlative metric, teams of policy writers, cyber underwriters, and FI leaders can examine this metric more closely to demonstrate correlation and establish use cases wherein the correlation is excellent or less so. Researchers can bring this identity metric within model development use cases and potentially surface use cases in which identity maturity can be demonstrated as a causative factor. Like the note in the previous section, this recommended cyber risk metric is envisioned as a sensitive business metric. It is not envisioned as a publicly available Fitch Rating (disclosure of which would benefit cyber criminals).

This metric is recommended as an important go-forward component within the critical discipline of cyber underwriting for FIs specifically and financial services broadly. Standards bodies such as NIST, in partnership with cyber risk professionals within financial services, seem best positioned to create this underwriting metric.

---

[19] "2nd Annual MIT/FRS Conference on Measuring Cyber Risk in the Financial Services Sector," Massachusetts Institute of Technology Internet Policy Research Initiative, January 16 and 17, 2024, accessed February 23, 2024, https://internetpolicy.mit.edu/cyberevent02/.

Conclusion

CISOs, CIOs, CTOs, chief risk officers, and chief identity officers at FIs, insurers, and other financial services firms:

- **Elevate the identity mindset:** Most businesses need more from digital identity than traditional IAM governing access and meeting compliance requirements. In partnership with other executives, CISOs can spearhead the mindset evolution toward identity investments that enable transformative outcomes for the business.
- **Seek strategic identity capabilities:** Besides enabling real business transformation, delivering elevated security assurance (zero trust solutions) is best achieved through many of these same solutions. Charge senior resources to investigate solutions included in this report and others.
- **Plan for long-term success:** Strategic business transformation requires a multiyear identity strategy closely aligned to business needs. A strong executive champion and winning some budget every year for strategic identity are two keys to success.
- **Introduce passkeys somewhere:** Capable solutions exist in the market. Start somewhere within the business. For some institutions, the workplace may present as a better case for initial passkey introduction, improving cyber risk for the enterprise while functioning as an incubation phase for offering passkeys to customers next.
- **Seek external domain expertise if needed:** Seasoned identity expertise is lacking throughout the market. Strategic identity is foundational to success for financial services firms. Many may require external experts to help establish a strategy and investment roadmap.

Identity vendors:

- **Partner to enable strategic business outcomes:** Long-term relationships require more than helping financial services firms meet compliance for MFA. Demonstrate the ability to deliver ROI and transformative business outcomes for CISOs and other executive leaders.
- **Intersect AI with identity:** AI has the potential to increase value for many areas of security. However, this analyst suggests that nowhere is this upside greater than aligning AI efforts to automate and enrich strategic identity capability. Invest in AI appropriately.

About Datos Insights

Datos Insights is an advisory firm providing mission-critical insights on technology, regulations, strategy, and operations to hundreds of banks, insurers, payments providers, and investment firms—as well as the technology and service providers that support them. Comprising former senior technology, strategy, and operations executives as well as experienced researchers and consultants, our experts provide actionable advice to our client base, leveraging deep insights developed via our extensive network of clients and other industry contacts.

Contact

Research, consulting, and events:

sales@datos-insights.com

Press inquiries:

pr@datos-insights.com

All other inquiries:

info@datos-insights.com

Global headquarters:

6 Liberty Square #2779
Boston, MA 02109

www.datos-insights.com

Author information

John Horn

jhorn@datos-insights.com