ISSN- 245-1142

International Journal of Humanities and Information Technology Volume 8, Issue 3, 2026

A Threat-Informed Framework for Secure Customer Identity (CIAM) Migration in Financial Services: Applying STRIDE, PASTA and Attack Trees to Legacy-to-Passwordless Transitions

Olabode Michael Soneye[1], Bolaji Mubarak Ayeyemi[2]

[1]EQ Bank, Ontario, Canada

[2]North Carolina A&T State University, Greensboro, NC, USA

Abstract

Financial institutions are replacing legacy customer authentication (passwords, one-time passcodes and hardware tokens) with phishing-resistant, passwordless Customer Identity and Access Management (CIAM) built on FIDO2 passkeys, OpenID Connect and sender-constrained OAuth 2.0 tokens. Research and standards describe the security of the target state well, but say little about the migration itself. During migration, legacy and modern identity stacks run side by side, customers hold mixed authenticators, and recovery, enrollment and federation paths multiply. This paper argues that the coexistence period is a distinct threat surface and that no single threat-modeling method covers it adequately.

Using a design-science approach, the paper makes four contributions. First, it derives a catalogue of sixteen migration-specific threats (MT-01 to MT-16), including authenticator downgrade, enrollment hijacking, recovery bypass, issuer mix-up and orphaned legacy endpoints. Second, it proposes the Phased Threat-Informed Migration Framework (PTIMF), which uses PASTA as the governing risk process, STRIDE for element-level analysis of phase-specific data flow diagrams, and attack trees for multi-step account-takeover goals. Third, it maps each threat to controls drawn from NIST SP 800-63-4, NIST SP 800-207 and the IETF OAuth security standards (PKCE, DPoP and RFC 9700). Fourth, an analytic coverage evaluation and an illustrative composite banking scenario show that the three methods are complementary: STRIDE surfaces most technical element threats, while process threats such as recovery abuse, policy drift and migration-themed phishing emerge mainly through PASTA and attack-tree analysis. The paper closes with phase-gate criteria for practitioners and a research agenda for empirical validation.

Keywords: customer identity and access management; passwordless authentication; FIDO2 passkeys; threat modeling; STRIDE; PASTA; attack trees; financial services; identity migration; Zero Trust

International Journal of Humanities and Information Technology (2026) **DOI:** 10.21590/ijhit.08.03.09

Introduction

Customer authentication is among the most attacked control surfaces in banking. Credential stuffing, phishing kits that relay one-time passcodes in real time, SIM-swap fraud and social engineering of contact-centre staff have all exposed the limits of knowledge-based and possession-based factors that can be phished. Regulators and standards bodies have responded by favouring phishing-resistant authentication. NIST SP 800-63B-4 makes phishing resistance a core property of higher authenticator assurance levels (NIST, 2025b). U.S. federal Zero Trust policy requires phishing-resistant multi-factor authentication for agency staff and directs agencies to offer it to the public (Office of Management and Budget [OMB], 2022). Financial supervisors, including the U.S. Federal Financial Institutions Examination Council (FFIEC, 2021) and Canada's Office of the Superintendent of Financial Institutions (OSFI, 2022), expect institutions to match authentication strength to transaction risk.

In practice, this means many banks are now migrating millions of retail and commercial customers from legacy authentication platforms to modern CIAM services. Typical targets are FIDO2/WebAuthn passkeys (W3C, 2021), OpenID Connect federation (Sakimura et al., 2014) and OAuth 2.0 authorization hardened with Proof Key for Code Exchange (PKCE; Sakimura et al., 2015) and Demonstrating Proof-of-Possession (DPoP; Fett et al., 2023). The security properties of these end-state technologies have been studied extensively

(Bonneau et al., 2012; Fett et al., 2016; Lyastani et al., 2020). The migration that connects the legacy state to the target state has received far less attention.

A CIAM migration is not instantaneous. For months, and sometimes years, two identity stacks coexist. Some customers have enrolled a passkey while others still rely on passwords and SMS codes. Account recovery must work for both populations. Federation bridges, token translation services and temporary migration APIs appear and later must disappear. Each of these transitional elements is a potential attack path. An attacker who can force a passkey-enrolled customer back onto a legacy password-and-OTP flow, or who can bind a new passkey to a victim's account through a weakly protected enrollment step, defeats the purpose of the migration while appearing compliant on paper.

Threat modeling is the established discipline for anticipating such risks at design time (Shostack, 2014). However, the main methods differ markedly in scope. STRIDE classifies threats against individual elements of a data flow diagram (DFD). PASTA (Process for Attack Simulation and Threat Analysis) is a seven-stage, risk-centric process that begins with business objectives (UcedaVélez & Morana, 2015). Attack trees decompose an attacker's goal into alternative and conjunctive sub-goals (Schneier, 1999). Systematic reviews report that each method has blind spots and that guidance on combining them is limited (Tuma et al., 2018; Xiong & Lagerström, 2019). Within identity security specifically, recent work has proposed identity-centric Zero Trust governance models (Ogbole et al., 2021) and privacy-centric security engineering for cloud systems (Okoruwa et al., 2020), but neither addresses the transition between authentication regimes.

This paper addresses that gap through three research questions:

- **RQ1.** What threats are specific to, or materially amplified by, the coexistence phase of a legacy-to-passwordless CIAM migration in financial services?
- **RQ2.** How do STRIDE, PASTA and attack trees differ in their ability to surface these threats, and how can they be combined into one workable process?
- **RQ3.** Which controls, mapped to current standards, reduce migration-phase residual risk to the assurance level intended for the target state?

The paper contributes (a) a migration-phase threat catalogue; (b) the Phased Threat-Informed Migration Framework (PTIMF), which assigns each method a defined role at each migration phase; (c) a threat-to-control mapping aligned with NIST SP 800-63-4, NIST SP 800-207 and IETF OAuth security guidance; and (d) an analytic evaluation of method coverage with an illustrative composite scenario. Section 2 reviews the background literature. Section 3 describes the research method. Section 4 presents the threat catalogue and Section 5 the framework. Section 6 reports the evaluation, Section 7 discusses implications and limitations, and Section 8 concludes.

Background and Related Work

CIAM in financial services

CIAM differs from workforce IAM in scale, user population and risk appetite. A retail bank may serve millions of customers who are not managed by the institution, use unmanaged devices and expect low-friction access. Commercial and lending platforms add partner organisations, delegated administration and machine-to-machine API access. CIAM platforms therefore combine registration, authentication, adaptive risk policy, consent and profile management, and token issuance for web, mobile and API clients. Directory services remain foundational to these platforms. Lessons from offline assessment of Microsoft Active Directory show that identity stores are security-critical systems whose misconfiguration propagates across the estate (Ladapo et al., 2018), and that efficient directory design underpins manageable access control (Ladapo et al., 2019).

Authentication sits within a wider set of banking controls. Quality assurance of secure digital banking platforms has been examined as a discipline in its own right (Daraojimba et al., 2025). AI-driven transaction monitoring has been compared with rules-based approaches for false-positive reduction in fintech (Kalu et al., 2024), and risk-typology frameworks have been proposed for monitoring cardholder accounts on prepaid and cross-border payment platforms (Kalu et al., 2023). These downstream fraud controls matter during migration because account-takeover attempts that slip past authentication must be caught by behavioural and transactional monitoring.

Passwordless and token-binding standards

The target state of most current migrations combines several standards:

- **FIDO2/WebAuthn and passkeys.** Public-key credentials scoped to the relying party's origin. Because the private key never leaves the authenticator and signatures are bound to the origin, a credential phished on a look-alike domain is useless (W3C, 2021). Usability studies suggest passwordless FIDO2 is broadly acceptable to users, but also identify concerns about account recovery and device loss (Lyastani et al., 2020).
- **OpenID Connect and OAuth 2.0.** Federation and delegated authorisation (Hardt, 2012; Sakimura et al., 2014). Formal analysis has identified attacks on OAuth such as mix-up attacks, where a client is confused about which authorisation server issued a response (Fett et al., 2016). Issuer identification was later standardised to counter mix-up (Meyer zu Selhausen & Fett, 2022).
- **PKCE and DPoP.** PKCE binds an authorisation code to the client instance that requested it (Sakimura et al., 2015). DPoP binds access and refresh tokens to a client-held key, so a stolen bearer token cannot simply be replayed (Fett et al., 2023). Mutual-TLS client authentication offers

an alternative sender constraint for confidential clients (Campbell et al., 2020).

- **OAuth 2.0 Security Best Current Practice.** RFC 9700 consolidates a decade of attack research into normative guidance, including deprecation of the implicit grant and requirements for exact redirect-URI matching (Lodderstedt et al., 2025).
- **NIST SP 800-63-4.** The 2025 revision of the U.S. Digital Identity Guidelines defines identity assurance, authenticator assurance (AAL1–AAL3) and federation assurance, and treats syncable passkeys and phishing resistance explicitly (NIST, 2025a, 2025b).

Threat-modeling methods

STRIDE classifies threats as Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege, applied to each process, data store, data flow and external entity in a DFD (Shostack, 2014). It is systematic and teachable, but it is element-centric: threats that arise from business processes, human behaviour or sequences of individually benign steps can be missed.

PASTA is a seven-stage risk-centric method: (1) define objectives, (2) define technical scope, (3) decompose the application, (4) analyse threats, (5) analyse weaknesses and vulnerabilities, (6) model attacks, and (7) analyse risk and impact (UcedaVélez & Morana, 2015). It links technical threats to business impact but is resource-intensive.

Attack trees represent an attacker goal as the root and decompose it into OR (alternative) and AND (required together) sub-goals (Schneier, 1999). They excel at multi-step attack chains and at showing which single control breaks the most paths, but they depend on the analyst choosing the right root goals.

DREAD (Damage, Reproducibility, Exploitability, Affected users, Discoverability) is a scoring scheme often paired with STRIDE. It has been criticised for subjectivity and inconsistent scoring between analysts (Shostack, 2014), which is why the framework in this paper uses it only as an optional input to a likelihood-impact assessment.

Systematic reviews conclude that threat-modeling research is fragmented, that methods are rarely validated empirically and that practitioners need guidance on tailoring and combining methods (Tuma et al., 2018; Xiong & Lagerström, 2019).

Related work on identity, risk and assurance

Several strands of work inform this study. Identity-centric Zero Trust governance positions identity as the primary control plane for enterprise security (Ogbole et al., 2021), consistent with the tenets of NIST SP 800-207 (Rose et al., 2020). Privacy-centric security engineering in cloud systems emphasises data minimisation and protection by design (Okoruwa et al., 2020), principles directly relevant to the bulk movement of customer identity data during migration. Insider-threat classification and risk modeling (Akeju et al., 2018) are pertinent because migration requires highly privileged service accounts and administrators. Risk-based cybersecurity assurance work has highlighted limits in data availability for assurance decisions (Fadayomi et al., 2019), a problem amplified when telemetry is split across two identity platforms. Continuous IT control monitoring has been proposed to modernise risk-based audit (Elebe et al., 2025), and risk-based testing has been advocated for complex enterprise systems (Fadero et al., 2024); both inform the phase-gate evidence requirements in Section 5. Research on password practices and authentication behaviour shows persistent weak habits even among trained staff (Onche & Ogbonna, 2022), reinforcing the case for removing shared secrets altogether. Finally, AI-augmented threat detection (Nlerum et al., 2026; Soneye et al., 2024) and CI/CD pipeline security controls (Obuse et al., 2024) provide detection and secure-delivery capabilities on which a migration programme depends.

Research gap

The literature addresses the security of the end-state authentication technologies and the general practice of threat modeling, but not the transitional risk of moving a large customer base between authentication regimes. No published framework, to the authors' knowledge, specifies which threat-modeling method to apply at which migration phase, or what evidence should gate progression from one phase to the next. This paper fills that gap.

Research Method

The study follows the design-science research paradigm, which produces and evaluates purposeful artefacts that address an identified organisational problem (Hevner et al., 2004). The design-science research methodology of Peffers et al. (2007) structured the work into six activities:

- **Problem identification and motivation.** Derived from the literature gap (Section 2.5) and from the first author's professional practice leading Design Security Risk Assessments for CIAM migrations in Canadian financial services.
- **Objectives of a solution.** The artefact must (a) cover threats across all migration phases, (b) assign a clear role to each threat-modeling method, (c) map threats to controls in current standards, and (d) define evidence that gates progression between phases.
- **Design and development.** The threat catalogue was built by deriving phase-specific DFDs for a generic legacy-to-passwordless migration, applying STRIDE per element, then extending the result with PASTA stage 1–2 business-process analysis and attack-tree decomposition of three attacker goals. Candidate threats were cross-checked against RFC 9700, NIST SP 800-63B-4 and published attack research (Fett et al., 2016; Ghasemisharif et al., 2018).
- **Demonstration.** The framework is applied to an illustrative composite scenario (Section 6.2). The scenario combines

Table 1: Migration phases

Phase	*Name*	*What changes*	*Characteristic exposure*
P0	Discovery and baseline	Inventory of legacy authenticators, clients, APIs, recovery paths and risk policies	Undocumented flows and "shadow" integrations
P1	Coexistence	New CIAM platform deployed; federation or token-translation bridge connects it to the legacy platform	Two token issuers, two session stores, two policy engines
P2	Progressive enrollment	Customers enroll passkeys and are linked to new identity records; legacy credentials remain valid	Enrollment, account linking and recovery become attack paths
P3	Cutover	Default login moves to the new platform; legacy authenticators restricted to fallback	Fallback and downgrade paths; surge in support and recovery requests
P4	Legacy decommission	Legacy platform, bridge and migration APIs retired	Orphaned endpoints, credentials and service accounts

common features of retail and commercial-lending CIAM migrations. It contains no proprietary, confidential or institution-identifying information.

- **Evaluation.** Following the Framework for Evaluation in Design Science (FEDS; Venable et al., 2016), the study uses an *ex ante*, artificial evaluation strategy suited to early-stage artefacts. It comprises an analytic coverage assessment of each method against the threat catalogue and a scenario walkthrough.

Communication. This article Positionality

The first author is a practising security architect. Practitioner insight improves relevance but introduces the risk of confirmation bias. To mitigate this, every threat in the catalogue is tied to a published standard or peer-reviewed attack study, and Section 7.3 sets out the empirical validation still required.

The Migration Threat Landscape

Migration phases

The analysis models a legacy-to-passwordless migration as five phases. The phases are generic; real programmes may overlap them or run them separately for different customer segments.

Threat catalogue

Table 2 lists sixteen threats that are specific to, or materially amplified by, the migration. Each is tagged with the phases in which it is most acute, its STRIDE category and its primary controls. Section 5.3 maps the controls to standards.

Three observations follow from the catalogue. First, the most consequential threats (MT-01, MT-02, MT-03) do not attack the new technology at all. They exploit the legacy paths that remain open around it. Second, several threats (MT-04, MT-10, MT-11) are integrity and governance failures rather than classic attacks, and are therefore easy to miss in a purely attacker-centric exercise. Third, MT-13 exploits the migration itself: customers who have been told to expect a change in login are more susceptible to lures that mimic it.

The Phased Threat-Informed Migration Framework (PTIMF)

Design principles

PTIMF rests on four principles derived from the solution objectives:

- **Risk-led governance.** PASTA provides the overall process, because migration decisions are business decisions: how long to tolerate coexistence, which segments to move first, and how much customer friction is acceptable.
- **Delta modeling.** Rather than one DFD of the end state, the team draws a DFD for each phase and analyses what has *changed*. STRIDE is applied per element to each delta, which keeps the work proportionate.
- **Goal-driven chaining.** Attack trees are built for a small set of high-value attacker goals, so that multi-step chains crossing legacy and modern components become visible.
- **Evidence-gated progression.** No phase begins until defined evidence shows the previous phase's threats are mitigated or formally accepted.

Method roles by phase

Table 3 shows how the three methods are combined. PASTA stages are mapped to phases; STRIDE and attack trees are used inside PASTA stages 4 and 6.

The three root goals used in this study are:

- **G1:** Take over a retail customer account during migration.
- **G2:** Obtain customer identity data in bulk.
- **G3:** Gain persistent access to commercial-lending APIs through a partner integration.

Figure 1 shows the attack tree for G1. It makes visible a point that element-level analysis tends to hide: three of the four top-level branches pass through legacy or transitional components rather than through the passkey itself.

Table 2: Migration-phase threat catalogue

ID	*Threat*	*Phases*	*STRIDE*	*Primary controls*
MT-01	Authenticator downgrade: attacker forces a passkey-enrolled customer onto the legacy password + OTP path	P1–P3	S, E	Per-account authenticator floor; no legacy fallback once a passkey is enrolled, except via high-assurance recovery
MT-02	Enrollment hijack: attacker uses a phished legacy session to bind their own passkey to the victim's account	P2	S	Step-up re-verification before binding; out-of-band notification; cooling-off period for high-risk actions
MT-03	Recovery as bypass: account recovery or contact-centre reset gives a weaker route than the authenticator it replaces	P2–P4	S, E	Recovery at equal or higher assurance; identity proofing per SP 800-63A-4; agent scripts and call-back verification
MT-04	Account-linking error: legacy and new identity records merged incorrectly, exposing one customer's data to another	P1–P2	T, I	Deterministic matching keys; reconciliation reports; human review of ambiguous matches
MT-05	Credential-store exposure: bulk export of legacy credential hashes or seeds during migration	P1	I	Just-in-time (lazy) migration at next login; encrypted transfer; no plaintext; short retention and verified destruction
MT-06	Issuer mix-up: a client accepts a token or response from the wrong of two authorisation servers	P1–P3	S	Issuer identification (RFC 9207); strict audience and issuer validation; one issuer per client where possible
MT-07	Bearer-token replay: stolen access or refresh token replayed from attacker infrastructure	P1–P4	S, E	Sender-constrained tokens (DPoP or mTLS); short token lifetimes; refresh-token rotation
MT-08	Authorisation-code interception on mobile or single-page clients	P1–P3	S	PKCE for all clients; exact redirect-URI matching (RFC 9700)
MT-09	Session-termination gaps: logout or revocation on one platform does not propagate to the other	P1–P3	E	Back-channel logout; shared revocation events; short bridge session lifetimes
MT-10	Risk-policy drift: adaptive MFA, velocity and device-risk rules not reproduced on the new platform	P1–P3	E, R	Policy inventory in P0; policy-as-code with equivalence tests; parallel-run comparison
MT-11	Audit discontinuity: authentication events split across platforms without correlation	P1–P4	R	Unified telemetry pipeline; common correlation identifiers; SIEM use cases for cross-platform anomalies
MT-12	Orphaned legacy endpoints reachable after cutover	P3–P4	E, D	Decommission checklist; external attack-surface scanning; credential and certificate revocation
MT-13	Migration-themed phishing: "re-enroll your account" lures exploiting customer expectation of change	P2–P3	S	In-app-only enrollment prompts; no links in migration emails or SMS; customer communication plan
MT-14	Availability and abuse surge: credential stuffing against new endpoints or overload during mass enrollment	P2–P3	D	Bot management; rate limits; capacity testing; staged enrollment waves
MT-15	Privileged migration accounts misused by insiders or compromised	P1–P4	E	Just-in-time privilege; dual control for bulk operations; session recording; prompt removal
MT-16	Partner and API client misconfiguration in commercial and lending integrations	P1–P3	T, I	Private-key JWT or mTLS client authentication; least-privilege scopes; partner onboarding review

STRIDE codes: S = Spoofing, T = Tampering, R = Repudiation, I = Information disclosure, D = Denial of service, E = Elevation of privilege.



Table 3: Method roles across migration phases

Phase	*PASTA stages emphasised*	*STRIDE (per element)*	*Attack trees*	*Gate evidence to exit phase*
P0 Discovery	1 Objectives; 2 Technical scope; 3 Decomposition	Baseline DFD of legacy flows	Define root goals (G1–G3)	Complete inventory of authenticators, clients, recovery paths and risk rules; risk appetite for coexistence signed off
P1 Coexistence	3 Decomposition; 4 Threat analysis	Delta DFD: bridge, second issuer, token translation	Extend trees with bridge and issuer nodes	Issuer validation, PKCE, DPoP/mTLS tested; unified logging live; credential-store handling approved
P2 Enrollment	4 Threat analysis; 5 Weakness analysis; 6 Attack modeling	Delta DFD: enrollment, linking, recovery	Full analysis of G1 (account takeover)	Step-up before binding; notifications; recovery assurance equals target AAL; linking reconciliation clean
P3 Cutover	6 Attack modeling; 7 Risk and impact	Delta DFD: fallback paths	Re-score trees with fallback restricted	Downgrade path closed for enrolled accounts; abuse and capacity tests passed; customer comms approved
P4 Decommission	7 Risk and impact (residual)	Delta DFD: removed elements	Confirm legacy branches are pruned	Endpoints unreachable; secrets and certificates revoked; migration accounts removed; residual-risk register closed

Figure 1. Attack tree for root goal G1. Branches are OR alternatives; leaves within the downgrade and enrollment branches must both succeed (AND). One control per branch removes that branch entirely.

Threat-to-control mapping

Table 4 maps each threat to controls in current NIST publications (Joint Task Force, 2020; NIST, 2025a, 2025b; Rose et al., 2020) and in IETF and OpenID specifications (Campbell et al., 2020; Jones et al., 2015; Jones & Bradley, 2022; Meyer zu Selhausen & Fett, 2022), so that teams can trace each mitigation to an authoritative source.

Risk scoring

PTIMF scores each threat on ordinal likelihood (1–5) and impact (1–5) scales defined during PASTA stage 1, so that scores reflect the institution's own risk appetite. Teams that already use DREAD can use its components as structured prompts when judging likelihood and impact, but the framework does not add DREAD scores together, given the known inconsistency of that practice (Shostack, 2014). Scores are recorded per phase. A threat's score is expected to fall as controls are introduced, and the phase gate requires every residual score above the agreed appetite to carry a named risk owner and an expiry date for the acceptance.

Evaluation

Analytic coverage assessment

Each threat in the catalogue was assessed for how readily each method surfaces it when applied as commonly practised. STRIDE is assumed to be applied to an end-state DFD, PASTA in full, and attack trees to goals G1–G3. The ratings are the authors' analytic judgement, made against the method definitions in Section 2.3. They are offered as a structured hypothesis for empirical testing (Section 7.3), not as measured results.

Three findings stand out. First, no single method surfaces more than half of the threats directly. Second, STRIDE and PASTA together surface 14 of 16 directly; the two they miss, authenticator downgrade (MT-01) and enrollment hijack (MT-02), are the threats that most directly defeat the purpose of the migration. Both are multi-step chains in which each step looks legitimate in isolation, which is exactly what attack trees are designed to expose. Third, the four threats STRIDE is unlikely to surface (MT-03, MT-10, MT-12, MT-13) are process, governance or human threats, or concern components that no longer appear in an end-state DFD. PTIMF's use of delta DFDs per phase is intended to recover MT-12 for STRIDE, while PASTA's business-objective stages capture the others.

Illustrative composite scenario

To demonstrate the framework, consider a composite mid-sized digital bank. It is migrating (a) retail online banking from a legacy platform using passwords plus OTP and hardware tokens to a cloud CIAM service offering passkeys and adaptive MFA, and (b) a commercial-lending portal to a developer-oriented CIAM service supporting custom flows and partner API access. The scenario is constructed for illustration and does not describe any specific institution.

P0 – Discovery. The PASTA stage 1 workshop sets objectives: eliminate phishable authenticators for retail customers within the programme timeline, while keeping login failure and contact-centre volume within agreed tolerances. The inventory finds a recovery route that is not in any architecture diagram: contact-centre agents can reset a customer's OTP

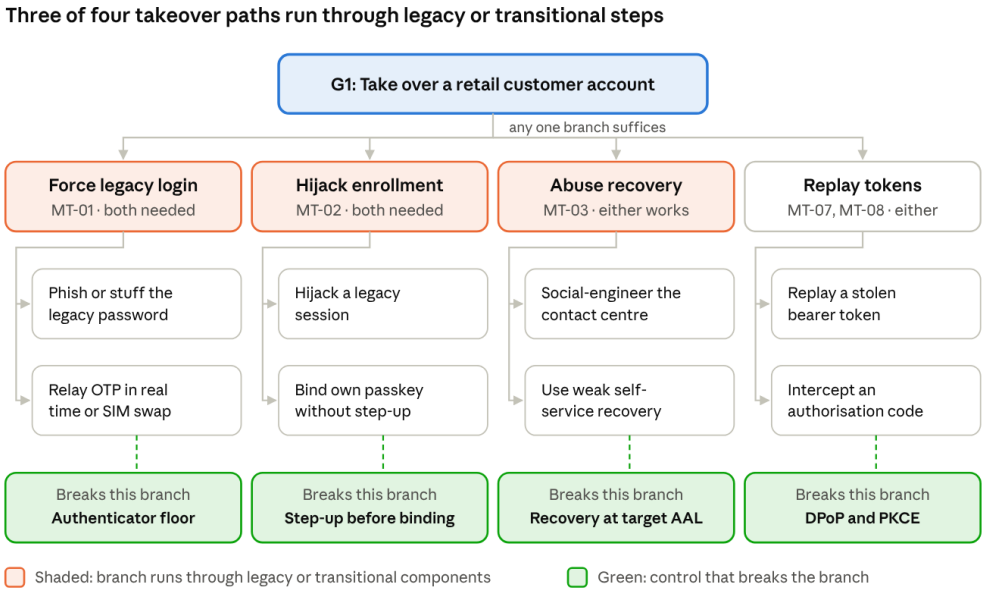


Figure 1: Attack tree for G1 (account takeover during migration)

device after knowledge-based questions. This becomes MT-03 and the C branch of the G1 tree.

P1 – Coexistence. The delta DFD adds a token-translation bridge so that legacy mobile app versions can call new APIs. STRIDE on the bridge's data flows raises issuer mix-up (MT-06) and bearer-token replay (MT-07). Controls: issuer identification, strict audience checks and DPoP-bound tokens for the new mobile app, with a sunset date for the bridge. Unified logging with a shared correlation identifier is made a P1 exit criterion (MT-11).

P2 – Enrollment. The G1 attack tree is completed. It shows that an attacker who phishes a legacy password and relays the OTP could, in the initial design, go straight to "add a passkey" without further checks. This is the AND chain in branch B of Figure 1. A single control breaks it: step-up verification at a higher assurance level before any authenticator is bound, plus an out-of-band notification and a short hold on high-risk transactions after binding. The same analysis shows that once a customer has a passkey, the legacy password-and-OTP path must not stay available as a silent fallback (branch A). The design therefore sets a per-account authenticator floor.

P3 – Cutover. Attack trees are re-scored with fallback restricted. PASTA stage 7 weighs the residual risk of the contact-centre recovery route against the cost of stronger identity proofing. The institution moves recovery to document-based remote identity proofing aligned with SP 800-63A-4 and adds call-back verification for agent-assisted cases. Customer communications commit to never sending links in migration messages, which addresses MT-13.

P4 – Decommission. The P4 delta DFD lists elements being *removed*. STRIDE is applied to the removal itself: what happens if an element is only partly removed? This produces a checklist covering DNS records, API gateway routes, service-account credentials, signing keys and certificates (MT-12, MT-15). External attack-surface scanning confirms that legacy endpoints are unreachable before the residual-risk register is closed.

Assessment against design objectives

Objective (Section 3)	*How PTIMF addresses it*	*Evidence in this study*
(a) Cover threats across all phases	Phase-specific delta DFDs and goal-driven trees	All 16 catalogue threats surfaced directly by at least one method (Table 5)
(b) Clear role for each method	PASTA governs; STRIDE per delta; attack trees per goal	Table 3; scenario walkthrough
(c) Map threats to standards	Control mapping	Table 4
(d) Evidence-gated progression	Exit criteria per phase; residual risk with named owner and expiry	Table 3; Section 5.4

Discussion

Theoretical implications

The study reframes CIAM migration security from a property

Table 4: Control mapping to standards

Threat	*NIST SP 800-63-4*	*IETF / W3C*	*NIST SP 800-207 tenet or SP 800-53 control*
MT-01 Downgrade	63B: phishing-resistant authenticators at AAL2/ AAL3	WebAuthn	800-207: dynamic, per-session access policy
MT-02 Enrollment hijack	63B: authenticator binding requirements	WebAuthn registration	800-53 IA-5 (authenticator management)
MT-03 Recovery bypass	63A: identity proofing; 63B: account recovery	—	800-53 IA-5, IA-12 (identity proofing)
MT-04 Linking error	63A: identity resolution	—	800-53 SI-10 (input validation), AU-6 (review)
MT-05 Credential-store exposure	63B: verifier storage requirements	—	800-53 SC-28 (protection at rest), MP-6 (sanitisation)
MT-06 Issuer mix-up	63C: federation assertions	RFC 9207; RFC 9700	800-207: authenticate every request
MT-07 Token replay	63C: bound assertions	RFC 9449 (DPoP); RFC 8705 (mTLS)	800-53 SC-23 (session authenticity)
MT-08 Code interception	—	RFC 7636 (PKCE); RFC 9700	800-53 SC-23
MT-09 Session gaps	63B: reauthentication and session management	OpenID back-channel logout	800-53 AC-12 (session termination)
MT-10 Policy drift	63B: risk-based authentication	—	800-207: policy engine; 800-53 CM-3 (change control)
MT-11 Audit discontinuity	—	—	800-207: collect telemetry; 800-53 AU-2, AU-6, SI-4
MT-12 Orphaned endpoints	—	—	800-53 CM-8 (inventory), SA-22 (unsupported components)
MT-13 Migration phishing	63B: phishing resistance	WebAuthn origin binding	800-53 AT-2 (awareness)
MT-14 Abuse surge	63B: rate limiting	—	800-53 SC-5 (denial-of-service protection)
MT-15 Privileged accounts	—	—	800-53 AC-6 (least privilege), AC-2 (account management)
MT-16 Partner misconfiguration	63C: federation assurance	RFC 7523 (JWT client auth); RFC 8705	800-53 SA-9 (external services), SR-6

of the end state to a property of the *trajectory*. An institution can deploy flawless passkey infrastructure and still be no safer if downgrade, enrollment and recovery paths remain open around it. This echoes the Zero Trust principle that every access request must be evaluated dynamically against policy (Rose et al., 2020; Ogbole et al., 2021): during migration, the policy itself is in flux, and the authentication path a customer takes becomes a risk signal in its own right.

The coverage analysis also adds to the threat-modeling literature. Earlier reviews called for guidance on combining methods (Tuma et al., 2018; Xiong & Lagerström, 2019). PTIMF offers one concrete answer for a specific, high-stakes context: a risk-centric process as the outer loop, element-level analysis of *changes* as the inner loop, and goal-driven trees for chains that cross old and new components.

Practical implications

For practitioners, the framework yields five actionable recommendations:

- **Treat fallback as a control decision, not a convenience.** Every legacy fallback path left open after passkey enrollment should be explicitly risk-accepted, with an owner and an expiry date.
- **Protect the binding moment.** Require step-up verification at or above the target assurance level before any new authenticator is bound to an account.
- **Raise recovery to the target assurance level.** Recovery is the authenticator of last resort and must not be the weakest one. Contact-centre procedures belong in the threat model.

Table 5: Method coverage by threat (● = surfaced directly; ◐ = surfaced only partly or with analyst prompting; ○ = unlikely to be surfaced)

Threat	*Stride*	*Pasta*	*Attack trees*
MT-01 Authenticator downgrade	◐	◐	●
MT-02 Enrollment hijack	◐	◐	●
MT-03 Recovery as bypass	○	●	●
MT-04 Account-linking error	◐	●	○
MT-05 Credential-store exposure	●	◐	◐
MT-06 Issuer mix-up	●	◐	◐
MT-07 Bearer-token replay	●	◐	●
MT-08 Code interception	●	◐	●
MT-09 Session-termination gaps	●	◐	◐
MT-10 Risk-policy drift	○	●	○
MT-11 Audit discontinuity	●	◐	○
MT-12 Orphaned endpoints	○	●	◐
MT-13 Migration-themed phishing	○	●	◐
MT-14 Availability and abuse surge	●	●	○
MT-15 Privileged migration accounts	◐	●	◐
MT-16 Partner misconfiguration	●	◐	●

- **Model what you remove.** Decommissioning is a phase with its own threats; orphaned endpoints, keys and service accounts are predictable findings.
- **Gate on evidence.** Phase exit criteria such as those in Table 3 give audit and risk functions something concrete to test, in line with moves toward continuous control monitoring (Elebe et al., 2025) and risk-based testing (Fadero et al., 2024).

For supervisors and auditors, the catalogue offers a checklist for examining migration programmes. Supervisory expectations for technology and cyber risk (FFIEC, 2021; OSFI, 2022) apply throughout the transition, not only to the target state. Downstream fraud analytics remain an essential safety net during coexistence (Kalu et al., 2024), and their tuning should anticipate the migration-specific attack patterns identified here.

Limitations and future research

This study has several limitations. First, it is a conceptual design-science contribution evaluated *ex ante*. The coverage ratings in Table 5 are analytic judgements by the authors and may reflect the first author's practitioner experience. Second, the demonstration uses a composite scenario rather than a documented case. Third, the threat catalogue is derived from one generic migration pattern; institutions using identity-provider consolidation, mergers or white-label platforms may face additional threats.

Future research should:

Table 6: Summary of coverage (count of 16 threats)

Method	*Surfaced directly*	*Partly*	*Unlikely*
STRIDE	8	4	4
PASTA	7	9	0
Attack trees	6	6	4

- Test the coverage hypothesis empirically by having independent teams model the same migration with each method, and compare the threats they find;
- Validate and extend the threat catalogue through a Delphi study with CIAM architects, fraud specialists and auditors (Okoli & Pawlowski, 2004);
- Conduct multi-case studies of completed migrations, measuring indicators such as fallback usage, recovery volumes and account-takeover rates before, during and after coexistence;
- Explore automation, for example "threat model as code" that regenerates delta DFDs from infrastructure definitions in CI/CD pipelines (Obuse et al., 2024), and AI-assisted detection of migration-phase anomalies (Nlerum et al., 2026; Soneye et al., 2024).

Conclusion

Moving customers to passwordless authentication is one of the most valuable security investments a financial institution can make. But the value is realised only when the legacy paths

around the new technology are closed. This paper has shown that the coexistence period of a CIAM migration creates a distinct set of threats, the most serious of which bypass the new authenticators rather than attack them. No single threat-modeling method surfaces these threats reliably. The Phased Threat-Informed Migration Framework combines PASTA's risk-centric process, STRIDE applied to phase-specific changes, and attack trees for multi-step takeover goals, and ties each phase to explicit exit evidence. The framework, threat catalogue and control mapping give practitioners a practical structure for secure migration and give researchers a set of testable propositions for empirical study.

Funding

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Conflict of Interest

The first author is employed as a security architect in the financial services sector. The views expressed are the authors' own and do not represent any employer or client. The authors declare no other conflicts of interest.

Data Availability

No datasets were generated or analysed. The scenario in Section 6.2 is a constructed composite and contains no confidential or institution-specific data.

References

[1] Akeju, B., Edivri, J., Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., & Abolaji, T. O. (2018). Conceptual model for insider threat classification and risk modeling in complex digital systems. *Iconic Research and Engineering Journals, 1*(9), 476–492. https://doi.org/10.64388/IREV1I9-1713778

[2] Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy* (pp. 553–567). IEEE. https://doi.org/10.1109/SP.2012.44

[3] Campbell, B., Bradley, J., Sakimura, N., & Lodderstedt, T. (2020). *OAuth 2.0 mutual-TLS client authentication and certificate-bound access tokens* (RFC 8705). Internet Engineering Task Force. https://doi.org/10.17487/RFC8705

[4] Daraojimba, R. E., Fadero, S., Oyesiji, S. O., & Okoli, I. E. (2025). Quality assurance for secure digital banking and electronic tax filing platforms. *Indian Journal of Environment & Development, 16*(1), 159–187.

[5] Elebe, O., Anunagba, C. O., Oyesiji, S. O., Ngonadi, U., & Fadero, S. (2025). An analytics-driven framework for continuous IT control monitoring and risk-based audit modernization in US organizations. *International Journal of Science, Technology & Society, 9*(3), 139–176.

[6] Fadayomi, O., Abolaji, T. O., Edivri, J., Ogbole, J. I., Okoruwa, P. O., & Akeju, B. (2019). Risk-based cybersecurity assurance and data availability: Limitations, advances and future research opportunities. *Iconic Research and Engineering Journals, 2*(12), 602–617. https://doi.org/10.64388/IREV2I12-1713779

[7] Fadero, S., Abdulwahab, A. I., Minoungou, T. F. T., Anene, U., & Kumuyi, O. (2024). Risk based testing in complex enterprise systems. *International Journal of Humanities and Information Technology, 6*(4), 275–311.

[8] Federal Financial Institutions Examination Council. (2021). *Authentication and access to financial institution services and systems*. FFIEC.

[9] Fett, D., Campbell, B., Bradley, J., Lodderstedt, T., Jones, M., & Waite, D. (2023). *OAuth 2.0 Demonstrating Proof of Possession (DPoP)* (RFC 9449). Internet Engineering Task Force. https://doi.org/10.17487/RFC9449

[10] Fett, D., Küsters, R., & Schmitz, G. (2016). A comprehensive formal security analysis of OAuth 2.0. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1204–1215). ACM. https://doi.org/10.1145/2976749.2978385

[11] Ghasemisharif, M., Ramesh, A., Checkoway, S., Kanich, C., & Polakis, J. (2018). O single sign-off, where art thou? An empirical analysis of single sign-on account hijacking and session management on the web. In *Proceedings of the 27th USENIX Security Symposium* (pp. 1475–1492). USENIX Association.

[12] Hardt, D. (Ed.). (2012). *The OAuth 2.0 authorization framework* (RFC 6749). Internet Engineering Task Force. https://doi.org/10.17487/RFC6749

[13] Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75–105. https://doi.org/10.2307/25148625

[14] Joint Task Force. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53, Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

[15] Jones, M., & Bradley, J. (2022). *OpenID Connect back-channel logout 1.0*. OpenID Foundation.

[16] Jones, M., Campbell, B., & Mortimore, C. (2015). *JSON Web Token (JWT) profile for OAuth 2.0 client authentication and authorization grants* (RFC 7523). Internet Engineering Task Force. https://doi.org/10.17487/RFC7523

[17] Kalu, A., Fadero, S., Pedro, O., & Mide-Ibrahim, O. (2023). Enhanced due diligence in prepaid and cross-border payment platforms: A risk-typology framework for cardholder account monitoring. *International Journal of Technology, Management and Humanities, 9*(4), 408–436.

[18] Kalu, A., Pedro, O., Fadero, S., & Mide-Ibrahim, O. (2024). AI-driven transaction monitoring in fintech environments: Comparative false-positive reduction across rules-based and machine-learning detection models. *International Journal of Science, Technology & Society, 8*(1), 92–122.

[19] Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2018). Lessons learned from offline assessment of security-critical systems: The case of Microsoft Active Directory. *Iconic Research and Engineering Journals, 2*(6), 277–299. https://doi.org/10.64388/IREV2I6-1717205

[20] Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2019). Implementation of Active Directory for efficient management of enterprise networks. *Iconic Research and Engineering Journals, 3*(4), 608–627. https://doi.org/10.64388/IREV3I4-1717206

[21] Lodderstedt, T., Bradley, J., Labunets, A., & Fett, D. (2025). *Best current practice for OAuth 2.0 security* (RFC 9700). Internet Engineering Task Force. https://doi.org/10.17487/RFC9700

[22] Lyastani, S. G., Schilling, M., Neumayr, M., Backes, M., & Bugiel, S. (2020). Is FIDO2 the kingslayer of user authentication? A comparative usability study of FIDO2 passwordless authentication. In *2020 IEEE Symposium on Security and Privacy*

(pp. 268–285). IEEE. https://doi.org/10.1109/SP40000.2020.00047

[23] Meyer zu Selhausen, K., & Fett, D. (2022). *OAuth 2.0 authorization server issuer identification* (RFC 9207). Internet Engineering Task Force. https://doi.org/10.17487/RFC9207

[24] National Institute of Standards and Technology. (2025a). *Digital identity guidelines* (NIST Special Publication 800-63-4). https://doi.org/10.6028/NIST.SP.800-63-4

[25] National Institute of Standards and Technology. (2025b). *Digital identity guidelines: Authentication and authenticator management* (NIST Special Publication 800-63B-4). https://doi.org/10.6028/NIST.SP.800-63B-4

[26] Nlerum, O., Fakinlede, F., & Ibrahim, B. (2026). AI-driven anomaly detection frameworks in critical infrastructure networks for proactive threat mitigation. *Journal of Engineering Research and Reports, 28*(6), 331–348. https://doi.org/10.9734/jerr/2026/v28i61931

[27] Obuse, E., Akindemowo, A. O., Ajayi, J. O., Erigha, E. D., Adebayo, A., Afuwape, A. A., & Soneye, O. M. (2024). A conceptual framework for CI/CD pipeline security controls in hybrid application deployments. *International Journal of Future Engineering Innovations, 1*(2), 25–47.

[28] Office of Management and Budget. (2022). *Moving the U.S. government toward zero trust cybersecurity principles* (Memorandum M-22-09). Executive Office of the President.

[29] Office of the Superintendent of Financial Institutions. (2022). *Guideline B-13: Technology and cyber risk management*. OSFI.

[30] Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., Abolaji, T. O., Edivri, J., & Akeju, B. (2021). Conceptual model for identity-centric zero trust architecture in enterprise security governance. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7*(5), 393–415. https://doi.org/10.32628/IJSRCSEIT

[31] Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: An example, design considerations and applications. *Information & Management, 42*(1), 15–29. https://doi.org/10.1016/j.im.2003.11.002

[32] Okoruwa, P. O., Fadayomi, O., Akeju, B., Edivri, J., Ogbole, J. I., & Abolaji, T. O. (2020). Conceptual model for privacy-centric security engineering in digital and cloud computing systems. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 6*(5), 371–389. https://doi.org/10.32628/IJSRCSEIT

[33] Onche, V. O., & Ogbonna, C. S. (2022). Password practices, authentication behaviour, and data-protection compliance among secretarial professionals in higher education. *International Journal of Multidisciplinary Research and Growth Evaluation, 3*(6), 1001–1015. https://doi.org/10.54660/.IJMRGE.2022.3.6.1001-1015

[34] Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

[35] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

[36] Sakimura, N., Bradley, J., & Agarwal, N. (2015). *Proof Key for Code Exchange by OAuth public clients* (RFC 7636). Internet Engineering Task Force. https://doi.org/10.17487/RFC7636

[37] Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., & Mortimore, C. (2014). *OpenID Connect Core 1.0*. OpenID Foundation.

[38] Schneier, B. (1999). Attack trees. *Dr. Dobb's Journal, 24*(12), 21–29.

[39] Shostack, A. (2014). *Threat modeling: Designing for security*. Wiley.

[40] Soneye, O. M., Tafirenyika, S., Moyo, T. M., Eboseremen, B. O., Akindemowo, A. O., Erigha, E. D., Obuse, E., & Ajayi, J. O. (2024). Conceptual framework for AI-augmented threat detection in institutional networks using layered data aggregation and pattern recognition. *World Journal of Innovation and Modern Technology, 8*(6), 197–227. https://doi.org/10.56201/wjimt.v8.no6.2024.pg197.227

[41] Tuma, K., Calikli, G., & Scandariato, R. (2018). Threat analysis of software systems: A systematic literature review. *Journal of Systems and Software, 144*, 275–294. https://doi.org/10.1016/j.jss.2018.06.073

[42] UcedaVélez, T., & Morana, M. M. (2015). *Risk centric threat modeling: Process for attack simulation and threat analysis*. Wiley.

[43] Venable, J., Pries-Heje, J., & Baskerville, R. (2016). FEDS: A framework for evaluation in design science research. *European Journal of Information Systems, 25*(1), 77–89. https://doi.org/10.1057/ejis.2014.36

[44] World Wide Web Consortium. (2021). *Web Authentication: An API for accessing public key credentials, Level 2* (W3C Recommendation). W3C.

[45] Xiong, W., & Lagerström, R. (2019). Threat modeling – A systematic literature review. *Computers & Security, 84*, 53–69. https://doi.org/10.1016/j.cose.2019.03.010