# The Identity Mismodeling Crisis: Rectifying B2C and Workforce IAM Misuse in B2B Ecosystems

Anuradha Karunarathna[1,*]

[1] WSO2

**Abstract**

As Business-to-Business (B2B) interactions in the digital world mature toward 2026, a critical architectural weakness has become increasingly visible: the systematic misclassification of external business entities within Identity and Access Management (IAM) models. Startups frequently leverage Business-to-Consumer (B2C) identity platforms to represent business customers, optimizing for speed and self-service but overlooking organizational hierarchies, delegated administration, and contractual access boundaries. Meanwhile, mature enterprises often manage partners, suppliers, and contractors within Workforce IAM frameworks, treating them as part of the employee population despite fundamentally different lifecycle drivers and governance realities. Both approaches create structural misalignment. The result is identity technical debt, over-provisioned access, fragile lifecycle controls, audit complexity, and expanding third-party risk exposure. B2B relationships are inherently diverse, ranging from distributors and resellers to partners, suppliers, and business customers. Each relationship type demands different onboarding rigor, authentication assurance, authorization granularity, delegated administration models, and self-service capabilities. This paper argues that B2B IAM is neither "B2C at scale" nor "Workforce for externals," but a distinct identity domain whose first-class subject is the external organization. We show how the mismodeling crisis manifests as recurring field-level failures, trace each failure to the same root cause, and present a vendor-agnostic reference blueprint that treats the organization as a first-class identity construct.

**Keywords**

B2B IAM, organization identity, delegated administration, identity federation, multi-tenancy, fine-grained authorization, third-party risk, Zero Trust, identity modeling



## 1. Introduction

Collaboration in the modern enterprise no longer stops at the organizational boundary. A single platform business may simultaneously serve corporate customers by delivering a SaaS product to those businesses, work with resellers that sell and act on behalf of those customers, integrate with suppliers and partners through APIs, and grant contractors scoped, time-bound access to internal portals. Critically, these third parties are typically not individuals but organizations in their own right. Each of these relationships requires authenticated and authorized digital interaction across organizational boundaries, and each is governed not by an employment relationship but by a contractual one between businesses.

The discipline that manages these relationships is B2B IAM. Yet in practice, B2B identity is rarely modeled on its own terms. When only a handful of business customers exist at selection time, they are folded into a B2C/Customer Identity and Access Management (CIAM) suite and represented as ordinary consumers. When only a handful of partners exist, they are folded into a Workforce/B2E suite and treated as quasi-employees. Both choices function until a third-party organization's IAM requirements stretch the model, or until the accumulated risk of the mismatch surfaces in an audit or a breach.

This paper takes a clear position: B2B IAM is a distinct identity domain whose first-class subject is the external organization, not the individual. Treating it as a variant of consumer or workforce identity is not merely an ergonomic inconvenience; it is a security and governance liability whose cost compounds silently over time.

*TDI 2026: 4th International Workshop on Trends in Digital Identity, April 20–21, 2026, Verona, Italy*

*Corresponding author.

anuradhak@wso2.com (A. Karunarathna)

https://www.linkedin.com/in/anuradha-karunarathna/ (A. Karunarathna)





CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

published 2026-09-06

The contributions of this paper are fourfold. First, we frame third-party identity as a high-stakes and worsening attack surface. Second, we characterize the mismodeling crisis by contrasting the three identity domains along the dimension that distinguishes them and show why collapsing B2B into either neighbor fails. Third, we catalogue the recurring field symptoms of mismodeling and trace each to its root cause, then present a vendor-agnostic reference blueprint that resolves them. Fourth, we analyze why correct tooling is still under-adopted, identify the standardization gap as the central obstacle, and offer recommendations for practitioners, vendors, and standards bodies.

## 2. The Stakes: Third-Party Identity as an Attack Surface

Two breaches a decade apart illustrate that third-party identity has been, and remains, a structural weakness in enterprise security.

In December 2013, attackers compromised a major retailer by first phishing credentials from a heating, ventilation, and air-conditioning (HVAC) vendor that held access to the retailer's network. From that foothold they reached the payment systems and exfiltrated approximately 40 million debit and credit card records along with personal data on roughly 70 million individuals [1]. The failure archetype here is the *over-privileged third party*: a vendor identity carried more access than its function required.

In February 2024, a healthcare payments processor was breached when attackers used a stolen employee credential to reach a third-party remote-access portal that had no multi-factor authentication (MFA) enabled. The intrusion affected an estimated 190 million individuals [2]. The failure archetype here is the *under-secured third-party access*: an external access path governed by weaker controls than internal systems.

These are not isolated incidents but instances of a steepening trend. Industry analysis reports that the share of breaches involving a third party roughly doubled year over year, reaching approximately 30 percent [3], while supply-chain breaches take the longest of any vector to identify and contain — on the order of 267 days [4].

What gives this trend its weight is the sheer size of the population involved. An enterprise survey found that while internal employees are the largest *single* group of users touching corporate networks, devices, and cloud resources (29%), non-employee external identities — partners, customers, vendors, and contractors — collectively account for the majority: nearly half of all users (48%) once corporate customers are excluded, and close to two-thirds (64%) once they are included [5]. The implication is direct: external identities are not an edge case appended to a workforce system but the larger share of the access surface, and the way an enterprise models the identities of external organizations is therefore not a back-office detail. It determines whether third-party access is governed as a first-class security concern or improvised at the edges of a system designed for someone else.

Correct modeling, in other words, is a control. The remainder of this paper argues that the prevailing modeling choices weaken that control.

## 3. Three Identity Domains, One Mismodeling Crisis

IAM has historically organized itself around two subjects. Workforce IAM emerged to manage internal employees and devices under an organization's direct administrative control. Consumer IAM emerged later to handle high-volume, self-service consumer identity, with emphasis on registration, consent, and personalized experience [6]. B2B IAM shares some scale and integration concerns with consumer IAM, but introduces a different set of requirements — governance across organizational boundaries, identity federation, contractual enforcement, and multi-level delegated administration — that arise specifically because the host must manage access for external organizations *without* assuming control over those organizations' own identity infrastructure [6].

The distinguishing axis is the *first-class subject.* In B2C/CIAM the subject is the individual consumer; in B2E/Workforce the subject is the internal employee; in B2B IAM the subject is the external organization,

**Table 1**
The three IAM domains by their first-class subject. B2B IAM is structurally distinct, not a scaled or externalized variant.

| Dimension | B2C / CIAM | B2E / Workforce | B2B IAM |
|---|---|---|---|
| First-class subject | Individual consumer | Internal employee | **External organization** |
| Unit of compartmentalization | The user | One enterprise (single tenant) | Many organizations, nestable (sub-orgs, regions) |
| Lifecycle owner | Self (self-registration) | Central HR / IT | Delegated to each organization's own admins |
| Structure | Flat / none | Single org, internal hierarchy | Multi-organization hierarchy |
| Authentication policy | One consumer journey | One corporate policy | Per-organization policy; per-app level of assurance |
| Identity provider | Platform-hosted + social | Single corporate IdP | BYOI — each org's own IdP via enterprise SSO |
| Authorization | Coarse (entitlements, consent) | RBAC over internal roles | RBAC + FGA/ReBAC scoped per org; access delegation |
| Branding / UX | Single brand | Single brand | Per-organization branding |
| Governance | Individual privacy & consent | Centralized IT governance | Centralized governance, decentralized enablement |

and individual users are meaningful largely through their affiliation with it. Table 1 contrasts the three domains along the dimensions that follow from this difference.

The common and superficially reasonable mental model collapses one column into another. "We have only a few business customers, so fold them into the consumer system." "We have only a few partners, so treat them like contractors in the workforce system." A third temptation is to reach for Identity Governance and Administration (IGA), whose provisioning, deprovisioning, and access-review machinery looks like a fit for handling a high volume of identities. But IGA is typically built on the assumption that it has access to a central repository of identities — precisely what does not exist when the identities belong to external organizations — and it generally does not address self-service or invitation-based onboarding, authentication, or single sign-on, all of which are central to B2B [6]. Each of these substitutions functions at first. The claim of this paper is sharper: each works only until a third party's requirements stretch the borrowed model, or until the accumulated risk of the mismatch surfaces in an audit or a breach. The next section makes that claim concrete.

## 4. Symptoms Observed in the Field

When B2B is modeled as B2C or workforce, the same failures recur across deployments. Each is best understood not as an isolated defect but as an artifact of representing the organization implicitly rather than as a first-class entity.

### 4.1. Partner onboarding takes days, and identities fragment

Because there is no delegated administration, every new seat at a partner organization becomes a help-desk ticket for the host: a request is raised, queued, security-reviewed, and finally granted, often over several days. Partners wait while deals stall, and the same individual accumulates separate credentials across separate portals, fragmenting their identity.

### 4.2. Partner leavers silently retain access

Lifecycle is owned centrally by the host, with no link to the partner's own workforce changes. When an employee leaves the partner organization, that change does not propagate to the host's IAM. Because external relationships are by nature more fluid than employment — contractors, seasonal staff, and the contracts themselves expire and renew — these orphaned accounts accumulate faster than internal ones, yet linger as standing or "birthright" privileges that expand the attack surface and are typically

**Table 2**
Each field symptom is an artifact of the wrong subject model; the resolving capability follows from treating the organization as first-class.

| Field symptom (§4) | Root cause — artifact of the wrong subject model | Resolving B2B capability (§5) |
|---|---|---|
| Onboarding takes days; identities fragment across portals | No delegated administration — every seat becomes a host help-desk ticket | Self-service or sales-led organization onboarding + delegated user lifecycle management to the third-party organization's admin |
| Partner leavers silently retain access | Lifecycle owned centrally, with no link to the partner's own workforce changes | Delegated lifecycle + enterprise SSO/Bring-Your-Own-Identity-Provider (BYOI) so deprovisioning propagates from the partner's IdP; access certifications |
| Flat user groups do not scale across many customers | Customers modeled as flat groups in one shared tenant; no hierarchy, no fine-grained authorization | Hierarchical organization management + fine-grained (ABAC/PBAC/ReBAC) authorization scoped per organization |
| Tenant-per-customer isolation–sharing dilemma | Each customer is a fully isolated tenant — duplicated config, no shared governance | Organization as the unit of compartmentalization + centralized governance / decentralized enablement |

discovered by an auditor rather than by the system [7]. Timely deprovisioning, not initial grant, is where the borrowed model fails most dangerously.

### 4.3. Flat user groups do not scale across many customers

Modeling each business customer as one more group in a shared tenant provides no parent–child hierarchy for sub-organizations, regions, or business units, and no native path to fine-grained authorization. Group-level customization becomes error-prone, and there is a standing risk of access bleeding across customer boundaries [7].

### 4.4. Tenant-per-customer creates an isolation–sharing dilemma

Spinning up a fully isolated tenant per customer achieves separation but duplicates configuration, duplicates user identities for any user who belongs to more than one organization, and removes shared governance — producing synchronization and operational overhead that grows with every new customer [7].

These four symptoms share one underlying cause, and the resolving capability in each case follows from treating the organization as first-class. Table 2 makes the chain explicit and serves as the bridge to the blueprint in Section 5.

## 5. A Reference Blueprint: The Organization as a First-Class Identity Construct

The corrective is not a longer list of patches but a change of primitive. B2B IAM requires a first-class identity construct for the organization — one that supports resource isolation *and* controlled resource sharing, scale *and* per-organization customization, centralized governance *and* decentralized enablement, simultaneously [7]. The following capabilities, stated vendor-agnostically, constitute a reference blueprint. They align with the capability set that analyst evaluations now treat as definitional for the B2B IAM market [6].

**Organization as the unit of compartmentalization** The organization — not the user and not a wholly separate tenant — is the boundary around which identity stores, policies, branding, and governance are organized. This resolves the isolation–sharing dilemma by making sharing and isolation properties of a single, governed structure rather than mutually exclusive deployment choices.

**Organization identity semantics** Organizations carry their own attributes: legal name, registration and legal-entity identifiers, verification status, address, domains, and subscription. Linking an organization to a verifiable identifier — for example, a Legal Entity Identifier (LEI) resolvable against an authoritative registry [8] — enables Know Your Business (KYB) checks and lets contracts, attestations, and service levels attach to the organization itself rather than to individual users [6].

**Hierarchical organization management** Built-in tenancy allows each customer or partner to be represented as a logical compartment that can nest sub-organizations, regions, or business units. Heterogeneity across organizations is the norm, not the exception, and the hierarchy is what makes per-organization customization and governance tractable at scale [7].

**Centralized governance, decentralized enablement** The host governs access to its application and API portfolio centrally while delegating day-to-day enablement to each organization. This is the organizing principle that reconciles the host's need for control with the partner's need for autonomy.

**Delegated user lifecycle management** Each organization's own administrators onboard and manage their users and sub-organizations, without the host assuming control over — or responsibility for — the partner's internal changes. Delegation must support multiple levels with failsafe mechanisms that prevent inappropriate or runaway delegation [6]. Beyond offloading administrative cost, delegation is itself a security control: a partner administrator removes a departing user immediately, rather than leaving the host to catch the change in a quarterly or semiannual access review — closing precisely the orphaned-access window described above.

**Enterprise SSO and BYOI** Each organization can authenticate its users through its own identity provider via standard federation. Many of the organizations an enterprise wishes to collaborate with already maintain their own identities, attributes, and authentication mechanisms; allowing them to "bring their own" identity provider both reduces the burden on the host's IT staff and lets joiner–mover–leaver events in the partner's directory propagate to the host, directly addressing the orphaned-account problem of Section 4 [6].

**Per-organization journeys, policies, and assurance** Authentication, registration, and security policies vary per organization, with the level of assurance governed per application. Partners and corporate customers are not uniform; their requirements vary with the trust relationship and with each third party's own identity maturity [7].

**Mandatory and discretionary access delegation** A single identity may act on behalf of multiple organizations with different entitlements in each. Mandatory delegation designates users to act for an organization; discretionary delegation lets users invite others to act on their behalf. Both require the organization to be a first-class subject of authorization.

**Fine-grained and relationship-based authorization** Role-Based Access Control (RBAC) alone is insufficient for the hierarchical, cross-organizational decisions B2B requires; Attribute-, Policy-, and Relationship-Based Access Control (ABAC/PBAC/ReBAC) are needed to express policies over organizational metadata, subject and resource attributes, and runtime context, and to support delegated administration over digital estates shared by many organizations [6]. Relationship-based authorization is particularly apt here because B2B permissions frequently follow graph-shaped relationships between

entities — users, groups, organizations, and contracts — and may hinge on context that is not strictly identity-related, such as the expiration date of a contract, a class of decision that conventional workforce or consumer models are not built to express.

The B2B world is diverse: some use cases demand full hierarchies with deep delegated administration and per-organization branding; others need only lightweight grouping or occasional cross-tenant access. Choosing a B2B IAM approach is therefore an architectural decision about how to model a specific ecosystem, not merely a procurement decision [7]. A practical modeling exercise asks, among other questions: what is the login experience per organization; can one identity access multiple organizations; do organizations need self-service and delegated administration; and are there per-organization branding or SSO requirements [7].

## 6. Why the Drift Persists

If dedicated B2B IAM capabilities exist, why do competent teams keep reaching for the wrong tools? The explanation is structural, not a matter of negligence.

**The market and its recognition are recent** Dedicated B2B IAM tooling consolidated only over the last several years, and independent analyst recognition arrived later still — the first dedicated analyst Leadership Compass for the B2B IAM market was published as an inaugural edition, and analyst coverage of partner/B2B IAM as a category is similarly recent [6]. Surveys indicate that replacing homegrown B2B systems or repurposed workforce IAM still drives a large share of new deals — evidence that the mismodeling described here remains widespread [6]. For much of the period in which these systems were built, teams had little choice but to improvise on top of consumer or workforce stacks.

**Reason 1: at selection time, the problem looks like B2C** When requirements are gathered during vendor evaluation, a clearly B2B business case often surfaces as a set of consumer-identity needs. The customer says they do not need delegated administration today; all organizations are expected to share one login journey; no one anticipates varying recovery flows or policies per organization. The needs that distinguish B2B — delegation, per-organization policy, hierarchy — are exactly the ones that appear only once the next enterprise onboarding, audit, or breach forces them into view.

**Reason 2: switching forces application-layer change — and the standards are missing** The identity-tool swap is the easy part; the application rewrite it triggers is what stalls adoption. Most systems treat a user's organization as business data, carrying it as a custom claim rather than as a first-class identity attribute, because no widely adopted standard defines how to convey an authenticated user's organization within ID or access tokens, and provisioning standards such as the System for Cross-domain Identity Management (SCIM) have no standardized way to carry organization context, so implementations diverge. Migration therefore forces changes to authentication flows, onboarding, and downstream applications, not just to the IAM layer. This is the single most consequential obstacle.

**Reason 3: pricing is blamed, but rarely decisive** B2B plans are commonly more expensive than B2C plans, and price is the usual explanation offered for choosing the cheaper, ill-fitting option. In practice, teams that clearly need B2B capabilities seldom forgo them on price alone; price becomes a factor mainly when the team does not yet perceive a current need for B2B-specific capability. By the time the need is undeniable, the cost of *not* having modeled B2B correctly — measured in stalled deals, audit findings, or breach exposure — exceeds the plan difference by orders of magnitude.

## 7. Implications and a Call to Action

The analysis above points to one structural conclusion and several practical ones.

**For practitioners** Evaluate for the B2B need you will have, not only the one visible at selection time. Treat the choice of identity model as an architecture decision: enumerate, per organization, the login experience, cross-organization access, delegated-administration, branding, and SSO requirements before assuming a consumer or workforce model will suffice. Where the ecosystem is genuinely B2B, model the organization as a first-class entity from the outset, even if only a few organizations exist today.

**For IAM vendors** Reduce the application-layer cost of correct modeling by exposing organization context. Since there is no proper standard, interoperable mechanisms improve the extensibility and customizability of how organization context is communicated in assertions. Analyst evaluations note that KYB, identity verification, and related governance functions remain under-supported and frequently require custom integration [6]. Closing those gaps natively lowers the barrier to doing B2B correctly.

**B2B IAM as a Zero Trust imperative** Third-party identity is where the breach curve is steepening fastest, and it is becoming more central still as workloads move to the cloud, where physical location loses meaning and identity becomes the primary control. In a recent survey, 53% of organizations named external identity access management as part of their plan to protect sensitive data in the cloud — close behind purpose-built cloud security tooling and encryption [5]. This emphasis is reinforced by a hard practical constraint: enterprises generally cannot install mobile-device-management, data-loss-prevention, or endpoint agents on the laptops and phones of users who are not their own employees, so governing how external identities authenticate and are authorized is often the only control surface available. An identity model that represents external organizations explicitly — with governed delegation, propagating lifecycle, per-organization assurance, and fine-grained authorization — is precisely the control surface Zero Trust requires at the organizational boundary. Solid B2B IAM is, in this sense, a missing piece of many enterprises' Zero Trust strategies rather than an optional convenience.

## 8. Conclusion

B2B IAM is neither "B2C at scale" nor "Workforce for externals." It is a distinct identity domain whose first-class subject is the external organization, and modeling it as a variant of consumer or workforce identity produces a predictable sequence of failures: slow onboarding, orphaned access, unscalable grouping, and an unresolved isolation–sharing dilemma, each traceable to the same root cause. Representing the organization as a first-class identity construct, with hierarchical management, delegated lifecycle, enterprise SSO, per-organization policy, and fine-grained authorization under centralized governance, resolves these failures by construction. The remaining obstacle is not capability but interoperability: until organization context can be conveyed by standard means, correct modeling will keep carrying an application-layer tax. Rectifying the mismodeling crisis is therefore both an architectural discipline for adopters and a standardization agenda for the community and, given where the breach curve is heading and how much of the access surface is now external, a security priority for both.

## Declaration on Generative AI

During the preparation of this work, the author used Claude (Anthropic) in order to: Grammar and spelling check, Paraphrase and reword. After using this tool, the author reviewed and edited the content as needed and takes full responsibility for the publication's content.

## References

[1] U.S. Senate Committee on Commerce, Science, and Transportation, A "kill chain" analysis of the 2013 target data breach, Majority Staff Report for Chairman Rockefeller, 2014. Phishing of an HVAC

vendor's credentials led to compromise of payment systems; approx. 40M card records and 70M individuals affected.
[2] U.S. Department of Health and Human Services, Office for Civil Rights, Breach reporting and public disclosures regarding the 2024 change healthcare cyberattack, 2024. Intrusion via a third-party remote-access portal without MFA; estimated 190M individuals affected.
[3] Verizon, 2025 Data Breach Investigations Report (DBIR), Technical Report, Verizon Business, 2025.
[4] IBM Security, Cost of a Data Breach Report 2025, Technical Report, IBM Security, 2025.
[5] S&P Global Market Intelligence, 451 Research, 2024 Data Threat Report, Technical Report, S&P Global Market Intelligence, 451 Research, 2024. Survey of security and IT professionals across financial services, manufacturing/industrial automation, energy and utilities, telecommunications, transportation, and trucking/shipping.
[6] KuppingerCole Analysts, Leadership Compass: Business-to-Business Identity and Access Management, Technical Report 80972, KuppingerCole Analysts AG, 2026.
[7] A. Karunarathna, The nightmare of modeling b2b iam with traditional iam solutions, Medium, 2025. URL: https://anuradha-15.medium.com/the-nightmare-of-modeling-b2b-iam-with-traditional-iam-solutions-fdb56cc4dd42.
[8] International Organization for Standardization, Iso 17442: Financial services — legal entity identifier (lei), 2020. See also the Global Legal Entity Identifier Foundation (GLEIF).