White Paper

Why CIAM Projects Fail

By Bruce Levis, Gregory Natran, Ed Therriault, Jim Lawson, and Guy Pensa

CitizenOne

https://citizenone.us
info@citizenone.us

Hard Lessons from Decades in the Field

If you're running a CIAM project, or about to, we hope this list helps you avoid becoming another cautionary tale.

Collectively, the five of us have been deep in the digital identity world for over 60 years, much of it centered around public sector service transformation. We've advised on, implemented, rescued, and post-mortemed more digital identity and CIAM (Customer Identity and Access Management) projects than we can count. We've seen what works. We've seen what really doesn't.

We've been in the rooms where executive teams are first told their flagship project is off the rails and we've been the ones quietly called in to salvage what could be saved. CIAM projects don't fail because people are lazy or unintelligent. They fail for reasons that are complex, recurring, and painfully predictable. We've categorized these reasons into five types.

Over the years, we've learned many lessons—sometimes the hard way. These experiences directly shaped how we rebuilt our CitizenOne solution from the ground up. We designed it to meet the unique challenges of public sector CIAM projects head-on, drawing from deep lessons learned in the field, with a solution built for real-world government realities.

#5 The Stats Midterm Trap

Ask any math or engineering student about their introductory statistics course and watch their face tighten. These are students used to abstract logic and heavy-duty calculations. They understand the material—or so they think. Then the first midterm hits and humbles them. Stats isn't about brute force math; it's about understanding and applying the right logic at the right time. It's a fundamentally different way of thinking.

CIAM is a lot like that.

> At a glance, CIAM seems simple. Authenticate users. Authorize access. Add MFA and SSO. Done, right? Not quite.

Especially in small and mid-sized public sector organizations, CIAM is often handed off to IT as "another project." But CIAM touches everything from user experience to citizen trust to regulatory compliance. And when teams treat it as "just SSO plus MFA," they miss critical dimensions:

- Empowering citizens with consent-based control over their identities
- Streamlining experience by enabling citizens to bring their own identity or authenticator
- Understanding levels of assurance by service risk category
- Managing progressive onboarding and multi-step identity verification
- Supporting diverse populations through flexible proofing
- Integrating without introducing new security vulnerabilities
- Meeting stringent privacy, consent, and accessibility standards
- Designing robust fallback pathways for account recovery
- Capturing actionable KPIs for service improvement

These outcomes underscore the effectiveness of CIAM solutions in transforming public sector digital services.

#4 If You Build It... They Might Not Come

Technical delivery is not success. Uptake is success.

> We've seen CIAM systems delivered on time, on budget, and functionally complete—and then watched them fail spectacularly because citizens simply didn't use them.

Common UX mistakes that kill CIAM adoption include:

- Cluttered, confusing login screens ("which account do I use?")
- Long, complex identity proofing processes
- Broken or inconsistent mobile experiences
- Switching citizens back to offline identity proofing ("print this form")
- Poor consistency across integrated services
- Unclear, intimidating consent language
- Lack of fallback options for password resets, device loss, or errors
- No onboarding support for new users
- No consolidated personal view of services, benefits, and status updates

UX research consistently shows that digital identity systems must feel intuitive, transparent, and fast. If citizens encounter friction, confusion, or mistrust, they will abandon the process. Investing in UX is not a luxury. It's survival.

#3 Ignoring Compliance and Cybersecurity Until It's Too Late

In public sector CIAM, compliance and cybersecurity are not box-checking exercises. They are living disciplines that must be involved from day one.

Compliance isn't just about privacy laws. It spans IT standards, procurement rules, accessibility requirements, and jurisdictional data sovereignty. Cybersecurity isn't just about firewalls—it's about credential lifecycle management, incident response, breach notification obligations, and ensuring the ongoing integrity of government services.

Failing to engage early creates enormous risk:

- Privacy Impact Assessments (PIAs) can reveal systemic non-compliance
- Credential policies may fail NIST or ISO standards
- Accessibility audits may find exclusionary design
- Legal reviews may reject user terms or consent models
- Internal audits may uncover governance gaps
- Security audits may reveal unacceptable vulnerabilities
- Sensitive citizen data could be exposed
- Cross-jurisdictional service integration may breach laws

> **This isn't theoretical. We've seen it firsthand. We've helped customers who got it right early avoid major issues. We've also come in to projects late, after these problems triggered major delays, public scrutiny, massive rework costs, or even total project shutdowns.**

Ignoring compliance and cybersecurity could—and often does—turn a promising project into a public sector cautionary tale. This issue alone could easily rank even higher on our list.

#2 Inadvertently Becoming a Software Vendor

Many government buyers believe they are purchasing a CIAM "product." Too often, they're actually buying a "platform"—and the distinction is critical.

Think of leading companies along the SaaS-to-PaaS spectrum:

- Office 365 sits at the pure SaaS end: fully functional, out of the box, no coding required.
- Wix and Squarespace move slightly rightward: primarily configuration with minor flexibility.
- Shopify moves further right: powerful but often requiring implementation partners for deeper customization.
- Many CIAM competitors sit even further right: offering platforms where, despite extensive capability lists, buyers must build user journeys, handle system hardening, design citizen UX, and integrate critical services themselves.
- At the extreme PaaS end, you're essentially buying a VM, application server, storage, memory—and building everything from scratch.
- Public sector buyers do not have the budget structures, staffing profiles, or operational flexibility to function like private sector software vendors. Nor should they try.

Governments exist to deliver public services—not to compete with Silicon Valley. Their resources are optimized for compliance, service delivery, and citizen engagement, not continuous product development, security patching, or feature release cycles. Expecting public institutions to act like agile software companies is a recipe for failure.

In practice, when public sector organizations buy platforms instead of finished solutions, they often find themselves responsible for:

- Defining and building onboarding and authentication workflows
- Designing and maintaining citizen-facing UX components
- Managing complex credential issuance, federation, and identity lifecycle
- Writing, hosting, and continuously updating legal statements and consent flows
- Handling upgrades, patches, new feature rollouts, and compliance audits

> **Suddenly, the organization is burdened with ongoing product management demands it was never structured or funded to handle. What seemed like a manageable purchase quickly becomes an expensive, fragile, and politically fraught product ownership scenario.**

This is exactly where many CIAM projects collapse under their own weight—and why it's critical to fully understand what you're buying before you sign the contract. When we built the new CitizenOne we had this in mind, and have positioned the solution closer to a Shopify in the Spectrum eliminating much of the technical and project risk.

#1 People and Power

This is the most dangerous and hardest-to-fix challenge.

In most governments, CIAM is initially owned by a centralized IT organization. That centralization often followed years when every department, agency, or utility had its own independent IT team and roadmap. Centralization brought efficiency—but it also created resentment and mistrust.

Worse, many programs and services are delivered by different agencies, ministries, or even legally distinct entities like utilities, public transit authorities, or state (or Crown in Canada) corporations. They have their own compliance departments, cybersecurity teams, program owners—and their own priorities.

When a central CIAM system is proposed, it is often met with deep skepticism:

- Agencies fear losing control over citizen relationships and data.
- Local IT teams fear marginalization.
- Program owners resist integration because "our needs are unique."
- Stakeholders weaponize procurement policies, technical standards, or governance processes to slow or stop rollout.

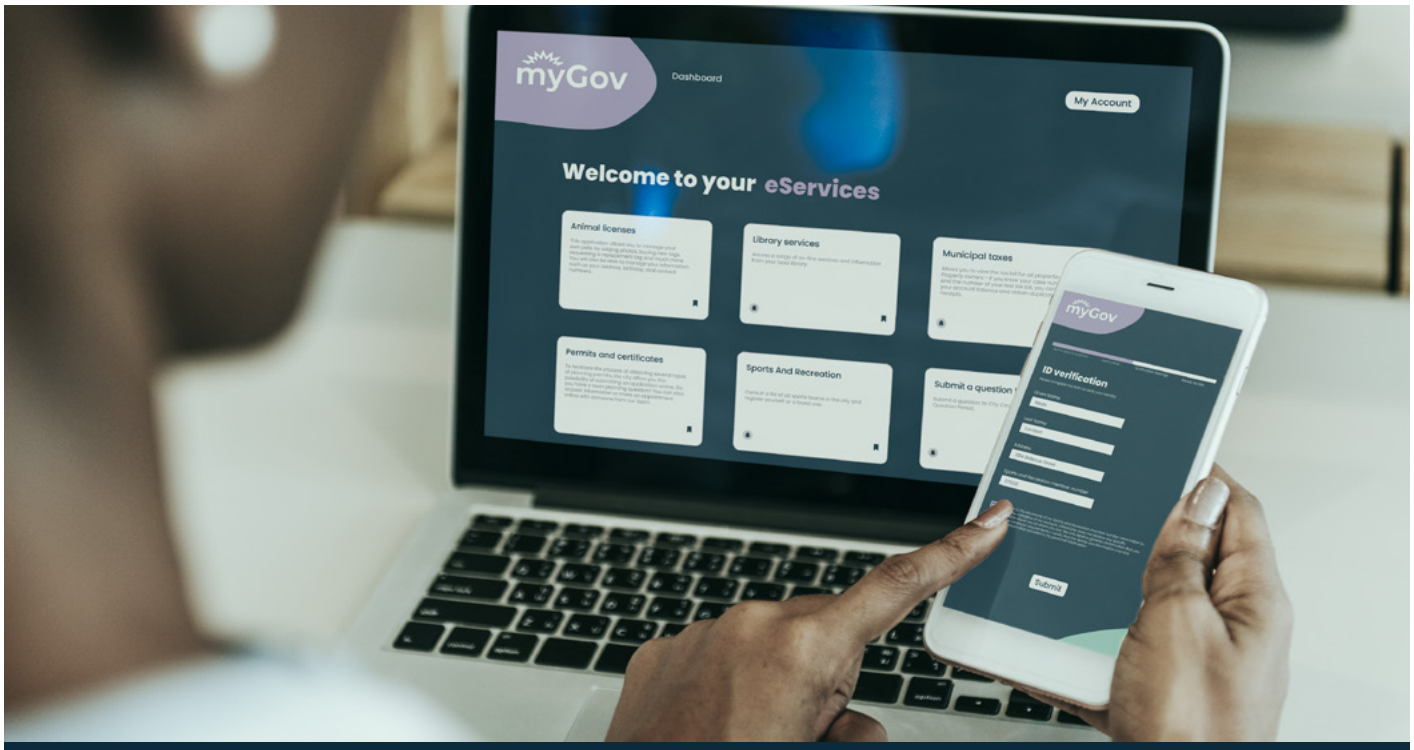
> **If people want to resist, they can—and they will—without ever getting formally blamed. They can "play by the book" and still kill momentum.**

When projects stumble, it's rarely the internal resistors who face consequences. It's external vendors, central IT, or the project leadership who get blamed.
Without world-class change management, relentless stakeholder engagement, and unwavering executive sponsorship, even the best CIAM system in the world can—and often does—fail.

Conclusion:
That's Why We Built CitizenOne

After decades of hard lessons, we didn't just build another identity platform. We rebuilt CitizenOne to fix these exact issues.

We joined standards bodies. We helped design national trust frameworks. We interviewed over 400 government organizations through IDC. We engaged deeply with frontline service providers. We partnered with research institutions experienced in carrier-grade systems.



CitizenOne is the first truly ready-out-of-the-box CIAM for governments—purpose-built to:

- Respect compliance, privacy, and cybersecurity from Day One
- Deliver citizen-first UX experiences
- Position our customers to avoid "accidental software vendor" traps
- Enable seamless, scalable integration
- Support program flexibility while protecting citizen trust

> We can't fix human nature. But we know how to work with it.

If you're starting a CIAM journey, we'd love to help you build it right—from the first decision to the final rollout.

Next Steps?
Questions?

Learn more about CitizenOne
or book a consultation
with one of our experts if you're
ready to explore how our solutions
can benefit your municipality.

© Copyright CitizenOne 2025