Questionnaire

CIAM Readiness Self-Assessment

A Tool for State, Provincial & Local Government Leaders Planning to Launch a CIAM Initiative

PORTAGE cybertech

portagecybertech.com
info@portagecybertech.com

CIAM Readiness Self-Assessment

A Tool for State, Provincial & Local Government Leaders

Before launching a CIAM initiative, use the checklist below to move from "planning an IT project" to "designing a resident service." This assessment helps identify where your agency stands and where the most immediate value can be unlocked.

Phase 1: Resident Experience (The "Friction" Audit)

Goal: Identify the pain points your residents actually face today.

Multiple Logins:
Does a resident need more than one username/password to interact with different departments in your agency?

☐ Yes ☐ No ☐ Not Sure

Manual Verification:
Do residents still have to present physical ID or mail paper documents to "prove" who they are for digital services?

☐ Yes ☐ No ☐ Not Sure

Help Desk Volume:
Are "password reset" or "account lockout" requests in your top 5 call center/support ticket categories? Or do your agents spend a lot of time pointing people in the direction of the service they need?

☐ Yes ☐ No ☐ Not Sure

Mobile Accessibility:
Can a resident easily log in and complete a transaction entirely from a smartphone?

☐ Yes ☐ No ☐ Not Sure

Phase 2:
Technical Environment (The "Silo" Audit)

Goal: Understand the complexity of your current identity landscape.

Fragmented Data:
Is resident data (names, addresses, emails) stored in multiple unconnected databases?

☐ Yes ☐ No ☐ Not Sure

Legacy Compatibility:
Do you have "anchor" applications that use older protocols (like LDAP or header-based auth) that struggle to talk to modern cloud apps?

☐ Yes ☐ No ☐ Not Sure

Security Gaps:
Are you currently able to enforce Multi-Factor Authentication (MFA) across all citizen-facing applications, or only some? Is it easy for the user?

☐ Yes ☐ No ☐ Not Sure

Integration Speed:
Does it take longer than 4 weeks to integrate identity into a new digital service or application?

☐ Yes ☐ No ☐ Not Sure

Phase 3:
Governance & Privacy (The "Risk" Audit)

Goal: Ensure compliance and resident trust are built-in, not bolted on.

Consent Management:
Do you have a centralized way for residents to manage their privacy and consent preferences and see what data is being shared?

☐ Yes ☐ No ☐ Not Sure

Audit Readiness:
Can you produce a single report showing all login activity for a specific resident across multiple services if requested for an investigation?

☐ Yes ☐ No ☐ Not Sure

Data Residency:
Do you know exactly where your resident identity data is stored (e.g., in-state, in-country, or offshore)?

☐ Yes ☐ No ☐ Not Sure

Fraud Detection:
Does your current system automatically flag suspicious login patterns (e.g., "impossible travel" or brute-force attempts)?

☐ Yes ☐ No ☐ Not Sure

Interpreting Your Results

Mostly "No" or "Not Sure":
You are in the "Legacy Stage."

Your primary risk is resident frustration and high operational costs. A "Wrap-Around" pilot on a single high-traffic service is your best first step.

A Mix of "Yes" and "No":
You are in the "Transition Stage."

You likely have some modern tools but lack a unified strategy. Focus on "Service-First" integration to bridge your silos.

Mostly "Yes":
You are in the "Optimization Stage."

Your goal should be "tell us once" functionality, exploring emerging technologies such as digital wallets and decentralized identity, and maximizing the value of existing investments.

Ready to take the next step?

Contact us to explore how a phased, public-sector-focused, strategic CIAM implementation can benefit your organization.

Portage CyberTech's solutions
https://www.portagecybertech.com/en/solutions/government-ciam

Book a consultation
https://www.portagecybertech.com/en/contact

Next Steps?
Questions?

Learn more about
Portage CyberTech's solutions.

Or book a consultation with one of our experts if you're ready to explore how our solutions can benefit your organization.