



# DECISION TIME CIAM: BUILD OR BUY?



---

Which approach to adopting Customer Identity & Access Management is right for your organisation?



## What to use this guide for

---

This succinct guide will help you decide, or present your decision to stakeholders, about whether to build Customer Identity and Access Management (CIAM) capabilities in house or buy the capabilities from an experienced CIAM provider.

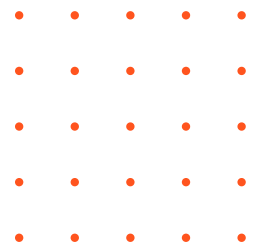
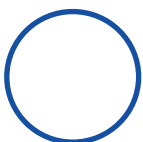
We will cover:

- What resources are required to build a CIAM solution in-house
- Questions to evaluate whether your specific organisation has the appropriate resources to build in-house (self build checklist)
- Potential risks of building a CIAM solution in-house, if you choose to do so
- The pros and cons of buying a solution from a CIAM vendor

If you want more detailed information about why CIAM investment matters, your choices around CIAM solution design, and other selection considerations, download the full [white paper on Build vs. Buy: CIAM](#).

If you're using this guide to pitch stakeholders and get budget allocation for CIAM, you'll probably also find [CIAM Investment and ROI - a Guide to the Value of CIAM projects](#) helpful.

As experienced CIAM specialists, the Ubisecure team is available to help you assess your CIAM requirements, and offer lessons learnt from similar projects. Contact us at [sales@ubisecure.com](mailto:sales@ubisecure.com).



## Building a CIAM solution

The concept of identity can be thought of as a collection of verified attributes – a set of name/value pairs that has to be corroborated before any system can trust that a person is who they say they are. This sounds straightforward. And in a closed system of trusted employees, IAM presents only a moderate technical challenge. However, there is a significant jump in complexity from traditional workforce-focused IAM to the much broader landscape of CIAM.

While it may be natural to think that a CIAM solution is one of many tasks that you can assign to your in-house technical team, our experience of offering identity management services since 2002 has shown us that the build process is not simple.

A self build process will likely divert resource away from your core business competency

A self-build process diverts resources from your team and slows down your progress on your main line of business. For example, if your organisation specialises in financial services, your efforts should be focused on providing that core proposition, not on spending time planning and implementing a niche technical project around identity management.

The same applies to almost all organisations who have a need for a CIAM solution – the work required is so specialised that a bought solution will be quicker and more robust than a custom-made alternative that is developed in house.

If your core business does not relate to access management, you will start to find complexity if you look to build your own CIAM solution. Naturally, there is a cost associated with outsourcing the job to an external provider, but this far outweighs the risk of doing the work in house and ending up with a system that may not be robust, standards compliant or scalable.

Building CIAM is a highly specialised skillset - make sure you have this in-house or you'll end up exposed to significant risk

Good IAM is essential to the running of a reliable digital service. A lack of investment in setting up the right identity management systems could have a long-term impact on your reputation and profitability. Failure to implement systems that achieve compliance with regulations and other security standards has the potential to put the viability of an entire business at threat.

Even the perceived benefit of the cost saving of doing identity management work in house is often a drawback in disguise. Unless you fully understand the complexity of the work needed, it is likely that you will underestimate the long-term cost of implementing and supporting your own CIAM solution.

BENEFITS OF BUILDING A CIAM SOLUTION	DRAWBACKS OF BUILDING A CIAM SOLUTION
<ul style="list-style-type: none"> <li>✓ You can control and customise every part of the identity management process.</li> <li>✓ Simple solutions may offer quick internal wins.</li> <li>✓ The intellectual property of the internal solution may be strategically important.</li> </ul>	<ul style="list-style-type: none"> <li>✗ High level of technical expertise required.</li> <li>✗ Complex and time-consuming to implement a custom system.</li> <li>✗ No guarantee of compliance with industry standards.</li> <li>✗ Scope creep – the risk of the project that never ends.</li> <li>✗ Support is critical and must be well resourced.</li> </ul>

## CIAM self-build checklist

Ask yourself these questions when considering whether to build your own CIAM solution:

- What size of team do we need?
- How long will it take us to implement a robust solution?
- Can we keep up with technical and compliance changes as part of our ongoing operation?
- Do we have expertise available immediately in case something goes wrong?
- Can we afford all of the implementation, testing and support costs?
- Can we afford to divert resources away from our core competencies?
- Can we produce an interoperable system that is faster, better or cheaper than a bought solution?
- Do we have the resources to follow changes in the legal landscape around personal data management?
- Do we have the resources to follow and react to security developments in the various related protocols?

## The costs and challenges of developing an in-house CIAM solution

The main issue we see with the build option is that the process is technical by nature and complex. Expertise is needed to configure the setup, and your team requires significant knowledge about the domain of identity management and security.

This complexity can have a significant effect on the speed of implementation of any in-house CIAM solution. For large software projects:

- 33% exceed their schedule.
- 66% exceed their budget.
- 17% underachieve on expected benefits.

Source: [McKinsey](#)

**Don't forget about ongoing maintenance and integration when projecting costs**

Building a CIAM solution is not a one-off project. If this work is done in house, your organisational responsibility will be to maintain the necessary IT expertise to support the identity management setup to ensure it functions as expected and interacts with other systems, including new systems you bring on board in future. This poses a significant technical challenge and can add a long-term cost to your IT budget.

Building and running your own CIAM solution involves costs such as data storage, data security, load balancing and the necessary staffing considerations – upskilling developers, managing teams, keeping training up to date, and so on. Good developers command high salaries, and a minimal enterprise-level development team may call for 6 or more such people. Consider also the need for 24/7 support for the enterprise, which would have to be managed in house, thereby adding a further financial burden.

**CIAM requires 24/7 support**

Some of the implementation costs depend on whether you opt for an on-premises data centre or a cloud solution (or hybrid). But in either case, the cost of developing your own CIAM solution is not to be underestimated.

Our experience tells us that, for most businesses and organisations, there is no compelling argument for building a CIAM solution in house. Consider the opportunity cost – the cost of choosing to develop your own in-house solution versus buying a CIAM solution. Picking this option means adding a non-core task to your workload, which comes at the expense of developing true expertise for your own domain.

Devoting resources away from your core services may not be a strategically wise move. Consider whether such an investment could be recouped elsewhere. For example, might it be possible to develop a platform that could be resold? Or could the development work lead to the creation of a new business arm? In most cases, these possibilities are unlikely to be realised. Rather than being an opportunity, such in-house development work tends to be a cost.

So, should any organisation ever build its own CIAM solution? Although we don't recommend this approach, there may be some scenarios where it could make sense:

- You have 10K+ employees and in-house expertise in identity management.
- You have security requirements so strict that you cannot use any third-party solution.

## Buying a CIAM solution

The alternative to building your own CIAM solution is to buy one from an identity services management provider. By purchasing a configurable CIAM product, you devolve the task to a specialist whose one and only function is to provide a robust, standards-compliant identity management solution. The result is that you can spend the time, money and energy on development and specialisation within your own organisation.

In the world of cybersecurity and IAM specifically, standards rule, and resource is expensive. In most cases, it makes little sense for your organisation to fight for expert development resource from a limited pool, when even general software development resource is scarce.

BENEFITS OF BUYING A CIAM SOLUTION	DRAWBACKS OF BUYING A CIAM SOLUTION
<ul style="list-style-type: none"> <li>✓ Pre-built, robust, highly tested and future-ready system.</li> <li>✓ No need to delay other projects and core services.</li> <li>✓ External support means no ongoing in-house support requirement.</li> <li>✓ Focusing on your main service will drive your business forward.</li> <li>✓ Compliance with relevant rules and regulations.</li> <li>✓ Better security – the CIAM solution provider abides by strict policies to keep data safe.</li> </ul>	<ul style="list-style-type: none"> <li>✗ Initial costs may seem high.</li> <li>✗ You may overlook in-house skills.</li> </ul>

## Summary

We believe that building your own CIAM solution is most often the weaker option when compared with buying a solution, especially when SaaS-based solutions, like [IDaaS](#), offer streamlined IAM functionality quickly, easily and at a lower cost.

The cost, complexity and long-term support burdens of such projects are easy to underestimate. Often, our Identity Platform software is selected to replace an in-house-developed solution that becomes unmanageable when significant team members leave the organisation.

Think carefully about the problem you solve for your clients and users. If security and identity management is part of your core proposition, building your own CIAM solution may make sense. However, for most organisations, your core

proposition relates to a different field. It therefore makes sense to focus on that core part of your business and to use an expert provider to handle all of the complexity of dealing with external identities. This results in a simplified operation and a reduction in risk to your organisation.

## Contact Ubisecure

---

If you would like to reduce your risk and remove the complexity of IAM, contact us to find out how we can help you implement the right CIAM solution for your organisation.

To learn more about Customer IAM and company identity solutions visit [www.ubisecure.com](http://www.ubisecure.com) or contact us at [sales@ubisecure.com](mailto:sales@ubisecure.com).

For examples of how companies like yours have utilised Ubisecure's CIAM solutions, please visit [www.ubisecure.com/customers](http://www.ubisecure.com/customers).



# About Ubisecure

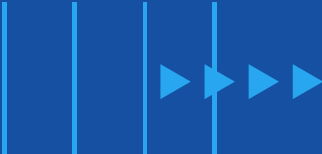




Ubisecure is a Europe-based Identity & Access Management (IAM) specialist and offers a comprehensive identity management platform deployed as IDaaS (Identity-as-a-Service) or on-premises software. The company is also GLEIF-accredited to issue Legal Entity Identifiers (LEI) via its RapidLEI service and has quickly become the global #1 LEI Issuer both in terms of volume and data quality.

As well as managing risk against data breaches, Ubisecure enables Zero Trust to greatly improve the security and experience of how users authenticate, register, access, engage and use the organisation's application, whether it's a web, mobile or a legacy service.

Enterprises use the Identity Platform to quickly implement use cases like single sign-on (SSO), multi-factor authentication (MFA), access management, authorisation and consent policies, advanced identity relationship management, login-as-a-service, and KYC/onboarding.

The platform has native support for a wide range of digital identities to enable real time identity verification and proofing, including Bank IDs, EU eIDs, mobile IDs, enterprise and social identities. Additionally, the RapidLEI service helps banks and FIs to manage and issue large volumes of LEIs to improve organisation-based authentication, meet compliance regulations, and provide better KYC/onboarding experiences for clients.



[www.ubisecure.com](http://www.ubisecure.com)  
[sales@ubisecure.com](mailto:sales@ubisecure.com)