IDENTRIO

2023

Building an effective IAM program



TABLE OF CONTENTS

01
Need for IAM

02
Types of IAM

03
Enterprise IAM

04
Enterprise IAM features

05
CIAM

06
CIAM features

07
Process

08
About Identrio

IDENTRIO

NEED FOR IAM

The need for an Identity and Access Management (IAM) system arises from the growing complexity of managing user identities, access privileges, and security in today's digital landscape. An effective IAM system can help organizations with the following:

- Improve security
- Detect and prevent data breaches
- Enhance end-user experience
- Ensure compliance
- Cost efficiency
- Reduce Helpdesk calls and tickets
- Centralized access management
- Auditing and reporting

34% of data breaches involve internal actors. IAM solutions provide centralized control and visibility over user access rights, allowing organizations to manage and monitor user privileges effectively, reducing the risk of insider threats. (Source: Verizon's 2020 Data Breach Investigations Report)

TYPES OF IAM

There are two types of IAM system:

- Enterprise IAM - Managing identities and access within an organization's internal ecosystem. It includes employees, contractors, partners, and other individuals associated with the organization.

- Consumer IAM (CIAM) - Managing identities and access for external users, specifically customers or consumers of an organization's products or services.

While there are similarities in terms of managing identities and access, the primary distinction between enterprise IAM and CIAM lies in the target audience, use cases, integration requirements, and focus on governance versus customer engagement.

ENTERPRISE IAM

- **Use Case**: To enable secure access to internal systems, applications, and resources for employees and authorized personnel. It emphasizes user provisioning, authentication, and authorization within the organizational network.

- **Integration**: Integrate with various on-premises and cloud-based applications, directories, and systems used within the organization, ensuring centralized access control and management.

- **Governance and Security**: Emphasis on strong governance, compliance, and security controls to protect sensitive corporate data and mitigate the risks of data breaches and unauthorized access.

- **Identity Lifecycle**: Manage end-to-end identity lifecycle events, including user provisioning, deprovisioning, access request workflows, and compliance-driven certifications and audits.

IAM FEATURES

Achieving a mature enterprise IAM system requires careful consideration of the following aspects:

- Automated onboarding and off-boarding
- Automated provisioning and de-provisoning
- Reconciliation of accounts and user access
- Data classification
- Password policies
- User lifecycle events
- Authentication
- Authorization
- Non-user/service account management
- Secondary accounts
- Self-Service capabilities
- Segregation of duties (SOD)
- API management
- Contractor management
- Application onboarding
- Universal ID
- Access Reviews
- Release Management
- Auditing and monitoring
- Compliance
- ROI metrics

CIAM

- **Use Case**: To provide a seamless and secure user experience for customers accessing digital platforms, such as websites, mobile apps, or online services. It facilitates customer registration, login, profile management, and personalization.

- **Integration**: Integrate with customer-facing applications, CRM systems, marketing platforms, and other systems that interact with customers to provide a unified and personalized user experience.

- **Scalability**: Focus on handling large volumes of customer identities, registrations, and authentication requests, providing high performance and scalability.

- **Customer Engagement:** Emphasizes on customer engagement and marketing capabilities, enabling organizations to gather customer insights, deliver personalized experiences, and manage consent and preferences.

- **Privacy and Consent Management**: Address privacy regulations, such as GDPR, by managing user consent, data subject rights, and providing transparency around data usage and sharing practices.

CIAM FEATURES

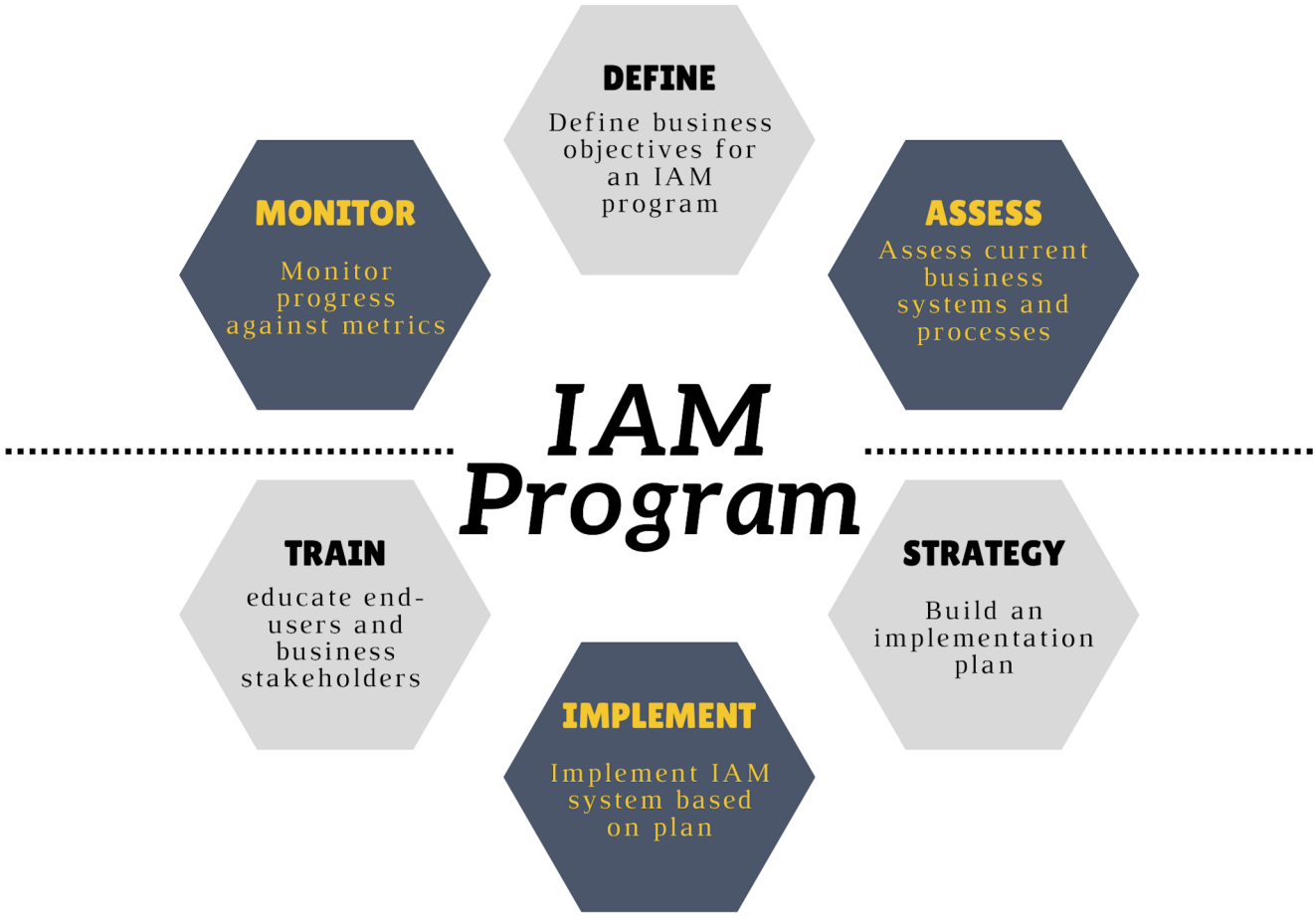
While enterprise IAM and CIAM share certain feature requirements, CIAM places a greater emphasis on user interface/user experience (UI/UX). The following are key features that a CIAM system should take into account:

- End-user experience
- Monitoring
- Data privacy and protection
- Performance and scalability
- Privacy and regulation compliance
- Progressive profiling
- Authentication
- Authorization
- Personalization
- Data synchronization
- First party data collection
- Consent management
- Self-service capabilities
- Auditing

PROCESS

Regardless of whether you are deploying CIAM or enterprise IAM, there are numerous factors to contemplate when implementing a new system. It is equally crucial to assess the current state of an existing IAM system, ensuring its continuous growth and alignment with the latest security trends.

Building an IAM program involves an iterative process to ensure its successful implementation.



Identrio can help at each step of the process to build an effective IAM program using our extensive knowledge and experience in IAM space

ABOUT IDENTRIO

Identrio offers comprehensive consultancy services and customized approaches in IAM governance, cyber and IT security, and user authorization to ensure our solutions are secure, flexible, and sustainable for your business.

Our offering includes:

01 — Professional Services

Our unparalleled professionalism and knowledge in IAM domain enable businesses to manage user access to systems and applications efficiently.

02 — Advisory & Assessment

Businesses can benefit tremendously from our Advisory & Planning Services, with our cybersecurity experts providing strategic guidance and planning for cybersecurity policies and practices.

03 — Cloud Security

In addition to our expertise, our comprehensive cloud security solutions provide robust authorization for cloud-based systems and applications, ensuring that businesses have peace of mind when protecting their critical data.

04 — Managed Support Services

Our Managed Support Services provide businesses with ongoing support and maintenance, ensuring they can continue to optimize core business operations.

Contact Us

www.identrio.com

info@identrio.com