Deloitte.

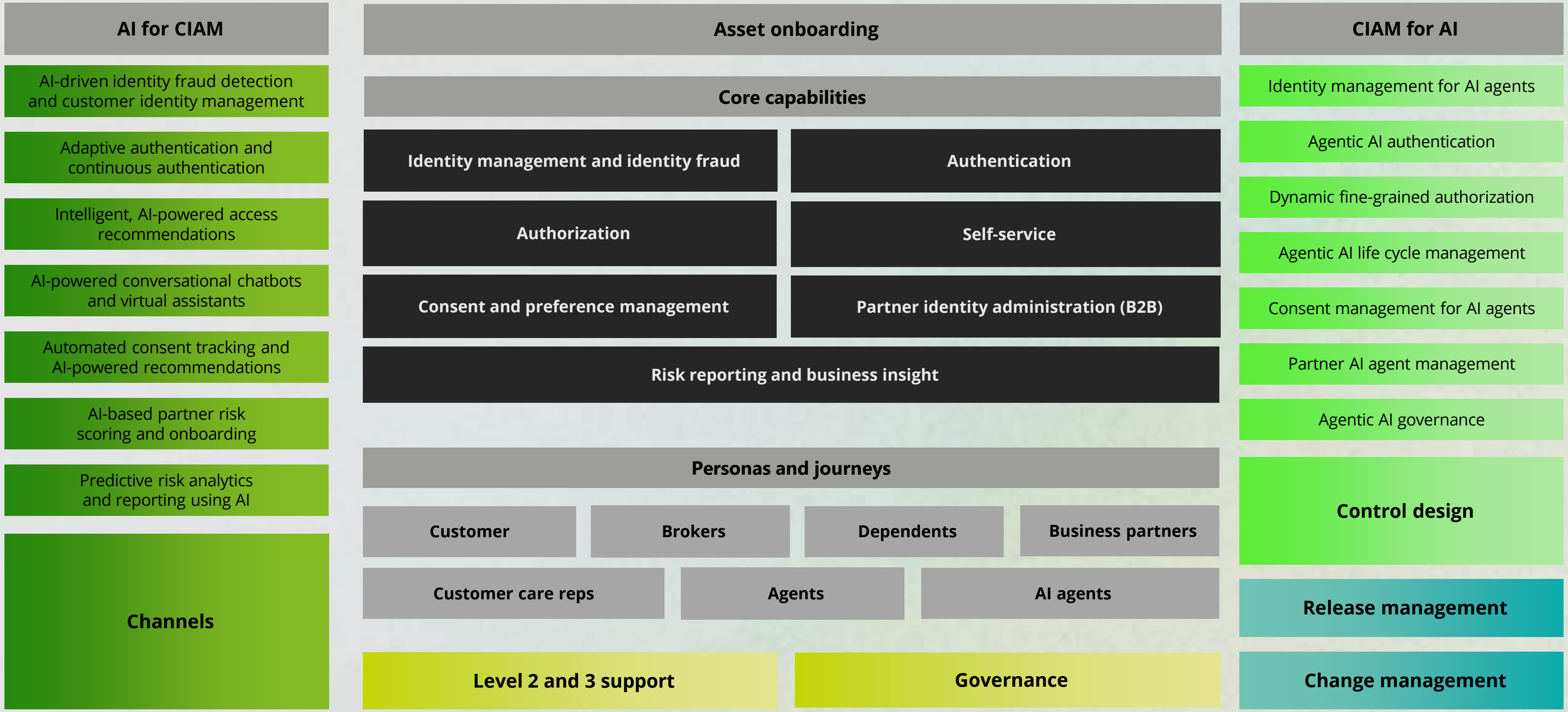
Reimagining the modern CIAM organization

As artificial intelligence (AI) and customer identity and access management (CIAM) evolve from foundational technologies to agentic intelligence, organizations that embrace these advancements can unlock accelerated strategic value, operational agility, and human-centric innovation.

AI and CIAM have rapidly evolved from basic automation and simple logins to strategic, nuanced, and powerful solutions such as agentic AI, passwordless authentication, and adaptive access. Today, integrating AI with CIAM can deliver personalized security, autonomous and contextual access, dynamic consent, proactive protection, and an effective user experience. To unlock the full value, companies should reimagine CIAM services including user registration, identity proofing, behavior-based authentication, and risk reporting, using AI protocols and controls. At the same time, broad CIAM practices are essential for secure adoption and governance of agentic AI so that new capabilities are both innovative and safeguarded.

The future of CIAM: Embracing AI

A blueprint for an AI-powered future: This model presents a strategic, AI-driven approach to CIAM, aligning people, technology, and workflows. It offers a practical roadmap to help organizations modernize cybersecurity, integrate AI-powered CIAM services, and strengthen defenses against emerging digital threats. The legend below identifies the new and evolved AI-enhanced services.



AI for CIAM

- AI-driven identity fraud detection and customer identity management
- Adaptive authentication and continuous authentication
- Intelligent, AI-powered access recommendations
- AI-powered conversational chatbots and virtual assistants
- Automated consent tracking and AI-powered recommendations
- AI-based partner risk scoring and onboarding
- Predictive risk analytics and reporting using AI

Channels

Asset onboarding

Core capabilities

- Identity management and identity fraud
- Authentication
- Authorization
- Self-service
- Consent and preference management
- Partner identity administration (B2B)
- Risk reporting and business insight

Personas and journeys

- Customer
- Brokers
- Dependents
- Business partners
- Customer care reps
- Agents
- AI agents

Level 2 and 3 support

Governance

CIAM for AI

- Identity management for AI agents
- Agentic AI authentication
- Dynamic fine-grained authorization
- Agentic AI life cycle management
- Consent management for AI agents
- Partner AI agent management
- Agentic AI governance

Control design

Release management

Change management

LEGEND

🟩	AI for CIAM
⬛	AI-enabled
🟩	CIAM for AI
🟨	Partial AI uplift with heavy human FTE
🟦	Deloitte Ascend™ for Cyber

Connect to accelerate

Contact our leaders to dive deeper into the blueprint and reimagine what's possible for your organization.

Mark Nicholson
Principal
Cyber AI GTM Leader
Deloitte & Touche LLP
manicholson@deloitte.com

Naresh Persaud
Principal
AI Transform/Digital Identity Leader
Deloitte & Touche LLP
napersaud@deloitte.com

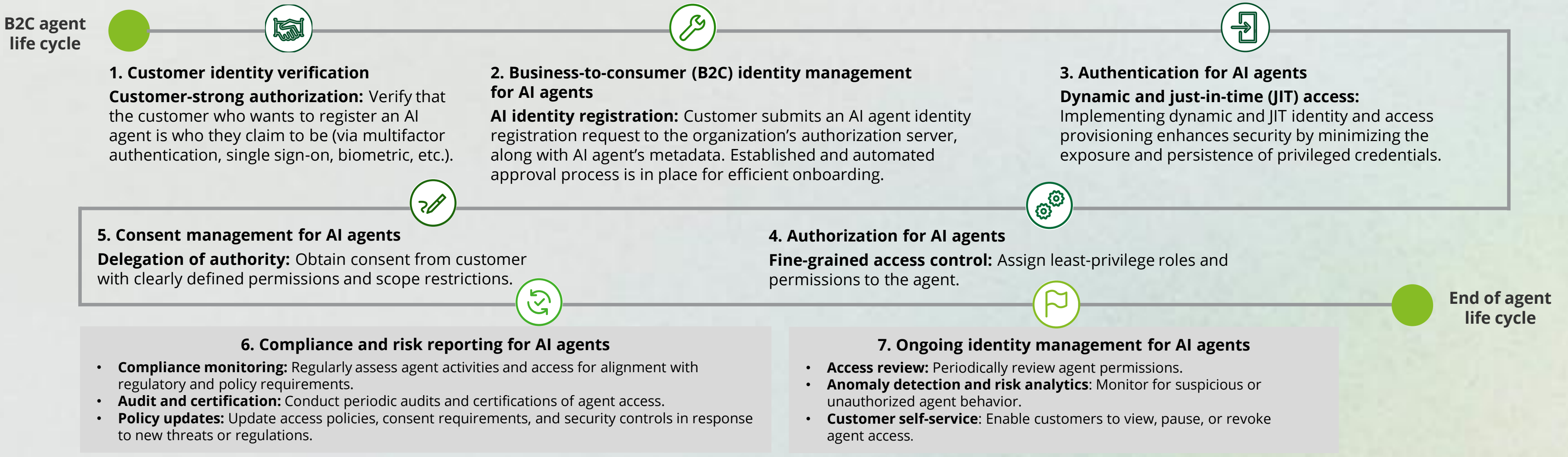
Anish Srivastava
Managing Director
US CIAM
Practice Leader
Deloitte & Touche LLP
anissrivastava@deloitte.com

Deepak Goyal
Senior Manager
Digital Trust & Privacy
Deloitte & Touche LLP
deepakgoya@deloitte.com

Steve Ruzzini
Senior Manager
Cyber AI GTM
Activation Lead
Deloitte & Touche LLP
sruzzini@deloitte.com

CIAM for AI: Safeguarding autonomous agents

Leverage CIAM to secure adoption and life cycle management of customer digital assistants and agentic AI, while governing AI to operate within defined privacy and access policies.



B2C agent life cycle

1. Customer identity verification

Customer-strong authorization: Verify that the customer who wants to register an AI agent is who they claim to be (via multifactor authentication, single sign-on, biometric, etc.).

2. Business-to-consumer (B2C) identity management for AI agents

AI identity registration: Customer submits an AI agent identity registration request to the organization's authorization server, along with AI agent's metadata. Established and automated approval process is in place for efficient onboarding.

3. Authentication for AI agents

Dynamic and just-in-time (JIT) access: Implementing dynamic and JIT identity and access provisioning enhances security by minimizing the exposure and persistence of privileged credentials.

4. Authorization for AI agents

Fine-grained access control: Assign least-privilege roles and permissions to the agent.

5. Consent management for AI agents

Delegation of authority: Obtain consent from customer with clearly defined permissions and scope restrictions.

6. Compliance and risk reporting for AI agents

- **Compliance monitoring:** Regularly assess agent activities and access for alignment with regulatory and policy requirements.
- **Audit and certification:** Conduct periodic audits and certifications of agent access.
- **Policy updates:** Update access policies, consent requirements, and security controls in response to new threats or regulations.

7. Ongoing identity management for AI agents

- **Access review:** Periodically review agent permissions.
- **Anomaly detection and risk analytics**: Monitor for suspicious or unauthorized agent behavior.
- **Customer self-service**: Enable customers to view, pause, or revoke agent access.

End of agent life cycle

AI for CIAM: Functional uplifts to achieve greater efficiency

Explore how harnessing AI and smarter solutions can reduce manual effort and accelerate results across key functions.

CIAM function	Uplift approach	Potential resulting impact
Assisted channel	Use **AI agents and biometrics** to automate customer authentication and anomaly detection.	**Reduction in contact center average handling time** by 20-30%, with increase in customer satisfaction[1]
Consent and preference management	Automate **regulatory policy enforcement**, **consent management**, **resource sharing**, and **compliance reporting**.	**Reduction in compliance breaches by 20-30%**, with increase in customer trust[1]
Identity fraud	Use AI to **analyze behaviors in real time**, detect risks, and automate fraud investigations.	**30% improvement** in detection rates and **50% reduction** in false positives[2]
Continuous authentication	**Continuously analyze user behavior** for anomalies and trigger adaptive responses in real time.	**Reduce account takeover** by 20-40%[1]
Fine-grained authorization	AI-driven access engine analyzes context and behavior to assess risk and **enforce policies in real time.**	**40% reduction in the manual labor** needed for routine policy maintenance[1]
Partner identity management	**Automate access reviews** to flag anomalies, continuously monitor for compromise, and use AI to assess risk in API and partner access.	**20% efficiency** in access reviews and **50% reduction** in false positives[2]

[1] Percentages are estimations based on recent project delivery for 10-15 organizations, ranging from 12-week implementation to 3-year operate engagements.

[2] Gartner: Case Study: Deep Fraud and Financial Crime Detection Built With Generative Adversarial Networks, Uri Lerner, Jasleen Kaur Sindhu (September 2024)

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com /us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.