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.

End of agent life cycle

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.

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)

Deloitte.

Reimagining the modern data protection function

In a business and technology landscape disrupted by generative artificial intelligence (GenAI), organizations could face increasingly complex data challenges.

The explosive growth of enterprise data has fueled a rapid expansion of data services (platforms, data processing, and analytics). In this complex and ever-expanding data landscape, organizations need to tackle rising frequency and impact of breach events, further exacerbated by agentic artificial intelligence (AI) solutions.

At the same time, regulatory scrutiny is intensifying around the globe. Multiple jurisdictions are enacting data protection requirements through a large set of global regulations regarding data governance, AI, and privacy. Noncompliance with these regulations often carry punitive actions.

Thus, organizations adopting GenAI solutions could face significant imperatives from customers, partners, and regulators to manage and maintain a broad security posture for trusted data handling, ultimately driving competitive advantages.

The future of data protection: Embracing AI

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

Function governance
- Vision and strategy
- Maturity assessments
- Function roadmap and architecture
- Staffing and budgeting
- Governance structures
- Training and awareness

Assurance and compliance
- Audit query walkthroughs
- Control testing and validation
- Regulatory reports and artifacts
- Compliance assurance

Core capability platforms

Data security posture management[1]	Data access and rights enforcement	Data loss prevention and cloud access security broker	Confidential computing/trusted enclaves
Classification and tagging	Encryption and key/certificate management	Data activity monitoring and flow telemetry	Data, model, and AI governance

Design and build
- Threat, risk, regulation, and compliance rationalization
- Control objective, scope, and use-case design
- Policy/ruleset design and tool configuration

Onboard
- Asset-specific control scope and mapping
- Nodes, connectors, and application programming interface (API) configuration
- Asset onboarding and validation

Operate
- Event/finding triage and disposition
- Misconfiguration and gap management
- Exception management and issue handling

Sustain
- Control refinement and enhancements
- Metrics and reporting
- Runbook development and maintenance

Data owner management

Asset owner mapping | Owner/steward engagement ("concierge") | Misconfiguration and gap remediation[2] | Data deletion/disposition | Context validation

Release and change management
- Program/project management
- Change management and governance
- Testing, quality assurance (QA), and release support
- Communication and documentation build

Tool management
- Tool enhancements and modernization
- System health monitoring
- Patching and upgrades
- Platform resiliency

Agentic AI capabilities
- Continuous data sensitivity review
- Data flow monitoring
- Policy enforcement
- Behavioral analysis
- Incident response orchestration
- AI runtime protection

Agentic AI enablement
- Machine learning (ML) security operations (SecOps)
- AI compliance
- AI trust
- AI performance evals

LEGEND

High-AI uplift opportunities | Independent software vendor tools | New services | Partial AI uplift opportunity | Deloitte Ascend™ for Cyber

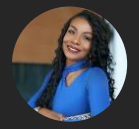
[1]Data Security Posture Management generally covers data discovery, semantic contextualization, misconfiguration detection, and reporting capabilities. [2]Misconfiguration remediation includes a variety of actions, such as key and certificate rotation, data access cleanup, data encryption/tokenization, DLP event blocking, file quarantine, classification label correction, and data deletion.

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 Transformation Leader
Deloitte & Touche LLP
napersaud@deloitte.com



Tanneasha Gordon
Principal
Data & Digital Trust Leader
Deloitte & Touche LLP
tagordon@deloitte.com

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

Protection for AI: Data, model, and AI protection for the enterprise

Protecting autonomous or semi-autonomous AI "agents" acting on behalf of users or organizations encompasses three major areas.

Area	Security concerns		Foundational priorities
Governance	Policies and controls	Capability roadmap	**Define:** Set controls using security standards for oversight and accountability. **Comply:** Adhere to industry regulations to maintain lawful AI operations and user trust. **Inventory:** Track agent identities, roles, and permissions for auditing and risk management.
	Regulatory compliance	Central policy management	
Visibility and baseline hardening	"Shadow AI" discovery	Data access and tool scope	**Find:** Discover and onboard AI agents to facilitate visibility, approval, and proper configuration. **Understand:** Monitor data flows and classify sensitivity for proper classification and tagging. **Harden:** Enforce security to protect data assets, model weights, and secure agent artifacts.
	Security policy enforcement	Data flow monitoring	
Runtime monitoring and response	Evaluation drift monitoring	Red teaming	**Monitor:** Collect telemetry, monitor data flows, and detect deviations and exfiltration. **Respond:** Remediate issues and orchestrate incident response to mitigate AI attacks. **Improve:** Use red teaming to test and refine security posture and AI build.
	Data exfiltration response	Input/output data guardrails	

AI for protection: Applying the blueprint for data, model, and AI protection

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

Area	Uplift approach	Potential impact
Data protection capabilities and controls	New capabilities unlocked by GenAI-empowered solutions, integrating data context and complex flows	**Continuously adapting controls, reducing risk through self-healing platforms**
Asset onboarding	Autonomous agents accelerating onboarding via scripts, API connectors, and health-check monitoring	**Consistent real-time asset coverage and streamlined onboarding in a frictionless manner**
Control workflow execution	Autonomous solutions driving context-driven event triage, remediation playbooks, summary narratives	**Decreased time-to-respond, false alerts, and consistent response playbook for reduced risk**
Control governance	Agentic solutions driving maturity assessments and feedback loops mapped to evolving requirements	**Continuous alignment and reduced efforts for maintaining capability maturity**
Data owner engagement	AI-driven approaches for inferring data ownership and self-service for business data owners	**Proactive engagement and reduced manual efforts for follow-up tasks**
Function governance	Use agentic approaches for trend monitoring and strategy refreshes	**Relevant strategy refreshes and synchronized plans with organizational changes**

Deloitte.

Reimagining the modern data privacy organization

The rapid evolution of artificial intelligence (AI), coupled with heightened security expectations and increasingly complex compliance landscapes, is fundamentally reshaping the privacy function. These converging forces are driving a reimagination of privacy strategy, governance, technology, and operations.

AI is rapidly transforming privacy management, offering new efficiencies that not only can streamline how organizations identify, classify, and protect sensitive data (especially across borders) but also can create opportunities to enhance consumer trust and drive business value. By automating processes such as risk detection, data subject rights management, and consent handling, AI can enable organizations to respond to customer needs with greater speed, accuracy, and transparency, which can reduce complaints and foster stronger relationships.

These advances help build consumer trust through greater transparency and stronger respect for privacy, allowing businesses to differentiate themselves in the marketplace and build loyalty—all while supporting scalable compliance frameworks and proactive governance that keep pace with evolving global regulations and help decrease financial and reputational risk.

The future of data privacy: Embracing AI

A blueprint for an AI-powered future: This model of the Data Privacy function and the underpinning services/processes provides the baseline to reimagine and map to an AI-driven model. The legend below identifies the new and evolved AI-enhanced services.

Governance and compliance

- Vision, strategy, and roadmap
- Privacy AI architecture
- Upskilling, training, and awareness
- Governance
- Control testing and validation
- Leadership reporting

Core capabilities

- Privacy by design/privacy risk assessments
- Data discovery and RoPA[2]
- Data subject rights
- Cookie management
- Consent and preference management
- Policy and notice management
- Digital compliance monitoring
- Incident management

AI-led privacy operations

- Data subject requests (DSR) automation
- Data transfer anomaly detection
- Privacy by Design (PbD) scanner
- PIA[3]/DPIA[4] execution, monitoring, and mitigation
- Automated RoPA[2] maintenance
- Metrics consolidation, aggregation, and reporting
- Website/app scanner for cookie and notice remediation
- Issue/complaints management and resolution

Privacy for AI

- AI privacy risk classification
- Data localization agent
- PET[8] integration with AI models
- Prompt and response scrubber agent
- Data minimization agent
- Data ingestion agent
- Data retention agent
- Purpose limitation agent
- Privacy drift detection
- Consent agent
- Privacy chatbot
- Data access governance agent
- Data manipulation and inference detection

Control design

- Regulatory and risk mapping
- Policy/ruleset design and tuning

Asset onboarding

- Agentic AI PbD[1] guidelines
- Asset and agentic AI registry

Level 2 and 3 support

- Misconfiguration remediation
- Troubleshooting
- Integration and code fixes
- Implementation scaling

Change management

- Executive communications
- Audience messaging
- Change governance support
- User guides and runbooks

Audit and compliance

- Testing and QA[5] support
- SLA[6] and performance
- [7]DevSecOps support
- Patching and upgrades

LEGEND

- **Privacy-specific AI uplift**
- **Privacy tech/software**
- **New privacy capabilities**
- **Partial AI uplift opportunity**
- **Deloitte Ascend™ for Cyber**

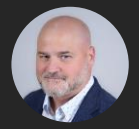
[1]Privacy by Design [2]Records of Processing Activities [3]Privacy Impact Assessment [4]Data Protection Impact Assessment [5]Quality Assurance [6]Service Level Agreement [7]Development, Security, and Operations [8]Privacy-Enhancing Technologies

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 Transformation Leader
Deloitte & Touche LLP
napersaud@deloitte.com



Dan Frank
Principal
Privacy Leader
Deloitte & Touche LLP
danfrank@deloitte.com

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

Privacy for AI: Advancing responsible autonomous agents

As AI agents impact operations, broad privacy keeps interactions secure and aligned.

Category	Agentic capability	Purpose
Back-end runtime privacy agents	Consent agent	Confirms data used for training or inference aligns with user consent and finds patterns of opt-ins/opt-outs driven by business events.
	Data access governance agent	Actively monitors user access to databases and repositories to detect and prevent unauthorized access.
	Purpose limitation agent	Enforces AI agents to operate within their defined purpose boundaries.
	Data localization agent	Enforces regional legal compliance for cross-border AI deployments.
Front-end runtime privacy agents	Prompt and response scrubber agent	Monitors interactions with large language models (LLMs) or autonomous agents to prevent malicious inputs and unintended personal information (PI) leaks.
	Data ingestion agent	Enforces privacy rules at the point of data intake (before training or inference).
Privacy monitoring agents	AI privacy risk classification agent	Continuously profiles and classifies AI models by privacy risk level.
	Privacy drift detection agent	Detects unintended privacy risks over time across the deployed models.

AI for privacy: Functional uplifts to achieve greater efficiency

Explore how harnessing AI and smarter solutions can redirect manual efforts to higher-level tasks and accelerate time to value.

Privacy function	Uplift approach	Resulting impact
DSR automation	Agents orchestrate the **end-to-end process execution**	**Free up Privacy full-time equivalents (FTEs) by 70%–80%*** resulting in direct savings
Automated RoPA maintenance	Agent maintains asset-based RoPA, **drastically reducing human workload**	**Live RoPA without dedicated FTE overhead,** freeing up bandwidth
Data transfer anomaly detection	Through metadata, rulesets, and registries, agents may **evaluate fitment of data transfers in real time**	**Instill stakeholder confidence** through authorized and justified data transfers
Metrics consolidation, aggregation, reporting	Metrics agent **provides real-time, audience-specific, template-driven reporting**	**Reduce operational overhead by 80%*** related to metrics and reporting
PbD scanner	Configure agents to scan the ecosystem and **identify violations against the rulesets**	Achieve automated PbD enforcement solving for **commonly de-prioritized** privacy goals
Issue management and resolution	Agent-driven issue **remediation planning and monitoring with minimal human reviews**	**Decrease of 50%–80%* enterprise time** to identify, triage, plan, and remediate issues

* Percentages are estimations based on recent project delivery for 8–12 organizations, ranging from 12-week implementations to 3-year operate engagements.