



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.

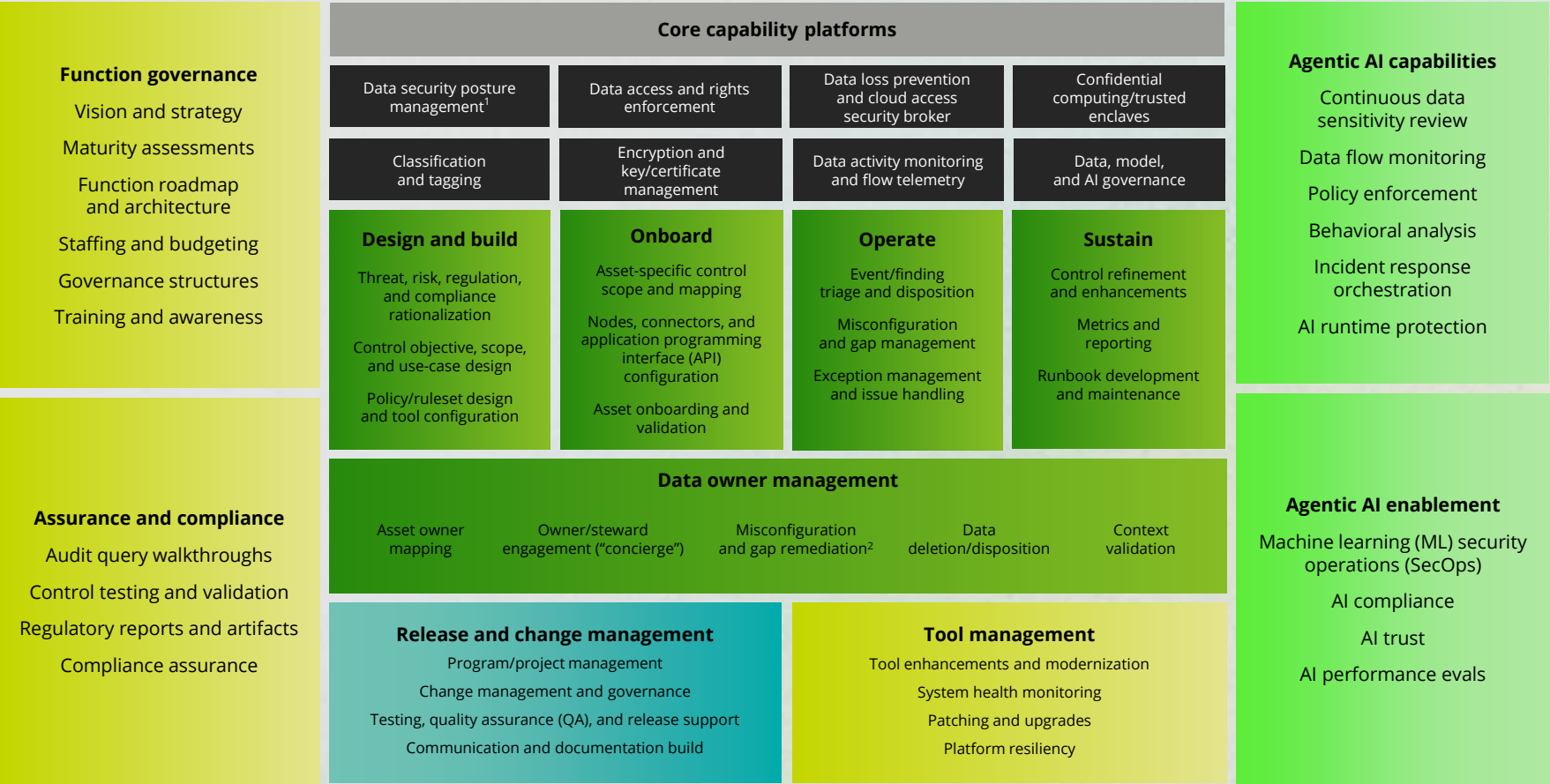
The explosive growth of enterprise data has fueled a rapid expansion of data services (platforms, data processing, and analytics). In this complex and ever-expanding data landscape, organizations need to tackle rising frequency and impact of breach events, further exacerbated by agentic artificial intelligence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



LEGEND

High-AI uplift opportunities

Independent software vendor tools

New services

Partial AI uplift opportunity

Deloitte Ascend™ for Cyber

¹Data Security Posture Management generally covers data discovery, semantic contextualization, misconfiguration detection, and reporting capabilities. ²Misconfiguration 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 data protection 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

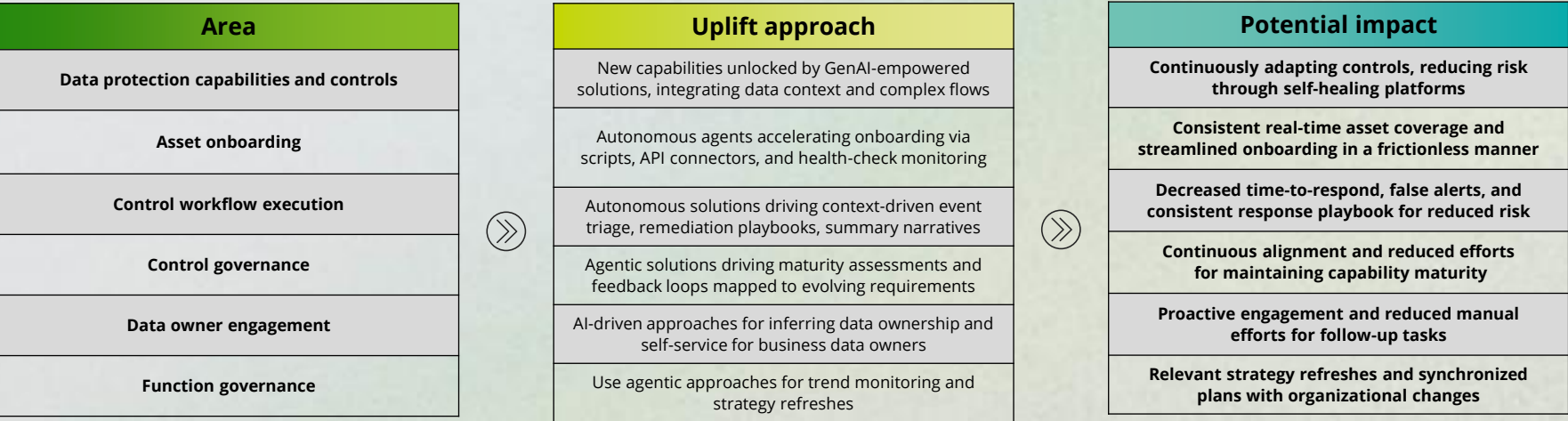
Protection for AI: Data, model, and AI protection for the enterprise

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.
	Regulatory compliance	Central policy management	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.
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.
	Security policy enforcement	Data flow monitoring	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.
Runtime monitoring and response	Evaluation drift monitoring	Red teaming	Monitor: Collect telemetry, monitor data flows, and detect deviations and exfiltration.
	Data exfiltration response	Input/output data guardrails	Respond: Remediate issues and orchestrate incident response to mitigate AI attacks. Improve: Use red teaming to test and refine security posture and AI build.

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.



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. Copyright © 2025 Deloitte Development LLC. All rights reserved.



Reimagining the modern data privacy organization

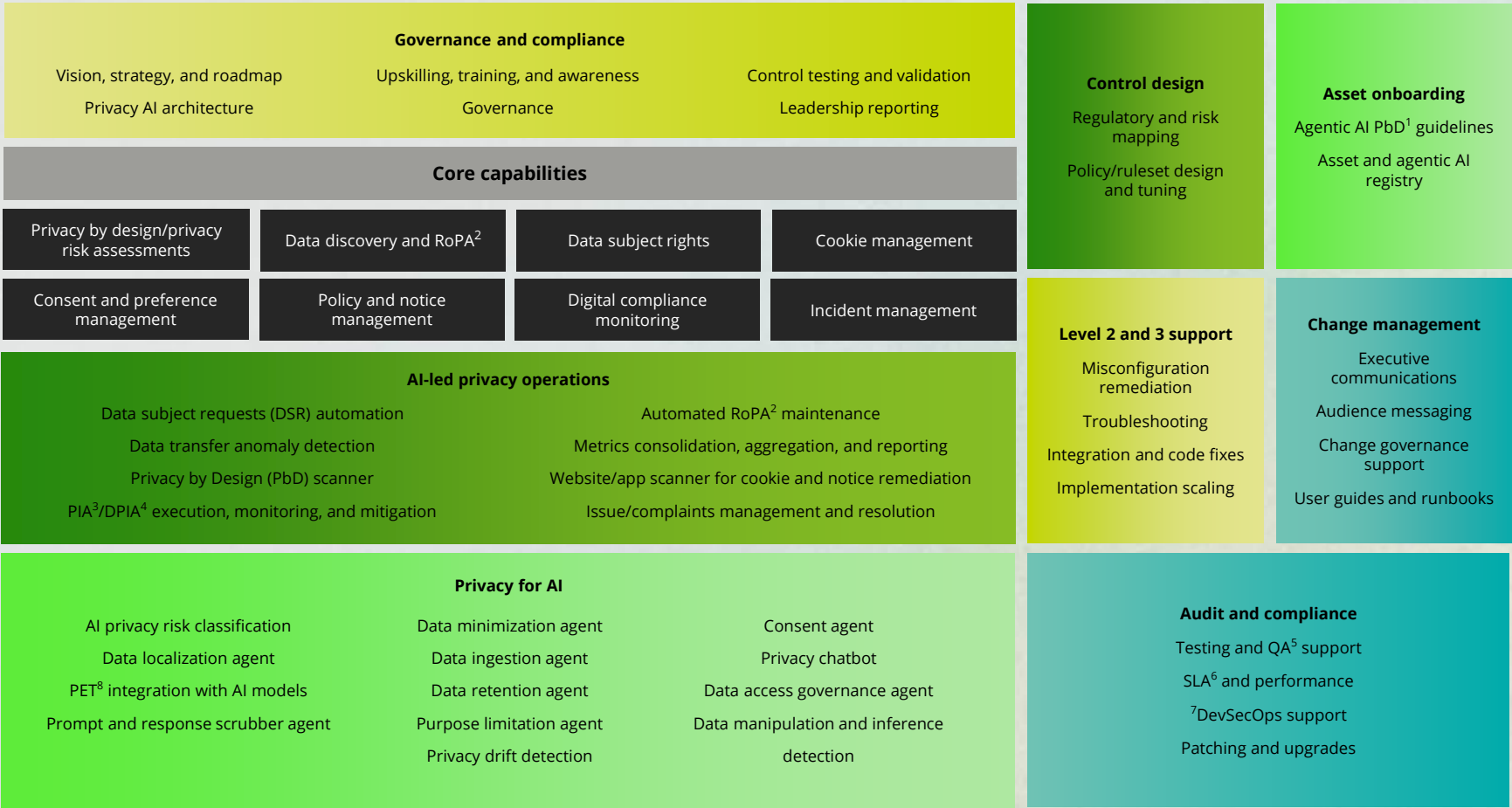
The rapid evolution of artificial intelligence (AI), coupled with heightened security expectations and increasingly complex compliance landscapes, is fundamentally reshaping the privacy function. These converging forces are driving a reimagination of privacy strategy, governance, technology, and operations.

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.



LEGEND

Privacy-specific AI uplift

Privacy tech/software

New privacy capabilities

Partial AI uplift opportunity

Deloitte Ascend™ for Cyber

¹Privacy by Design ²Records of Processing Activities ³Privacy Impact Assessment ⁴Data Protection Impact Assessment ⁵Quality Assurance ⁶Service Level Agreement ⁷Development, Security, and Operations ⁸Privacy-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. 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. Copyright © 2025 Deloitte Development LLC. All rights reserved.