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.

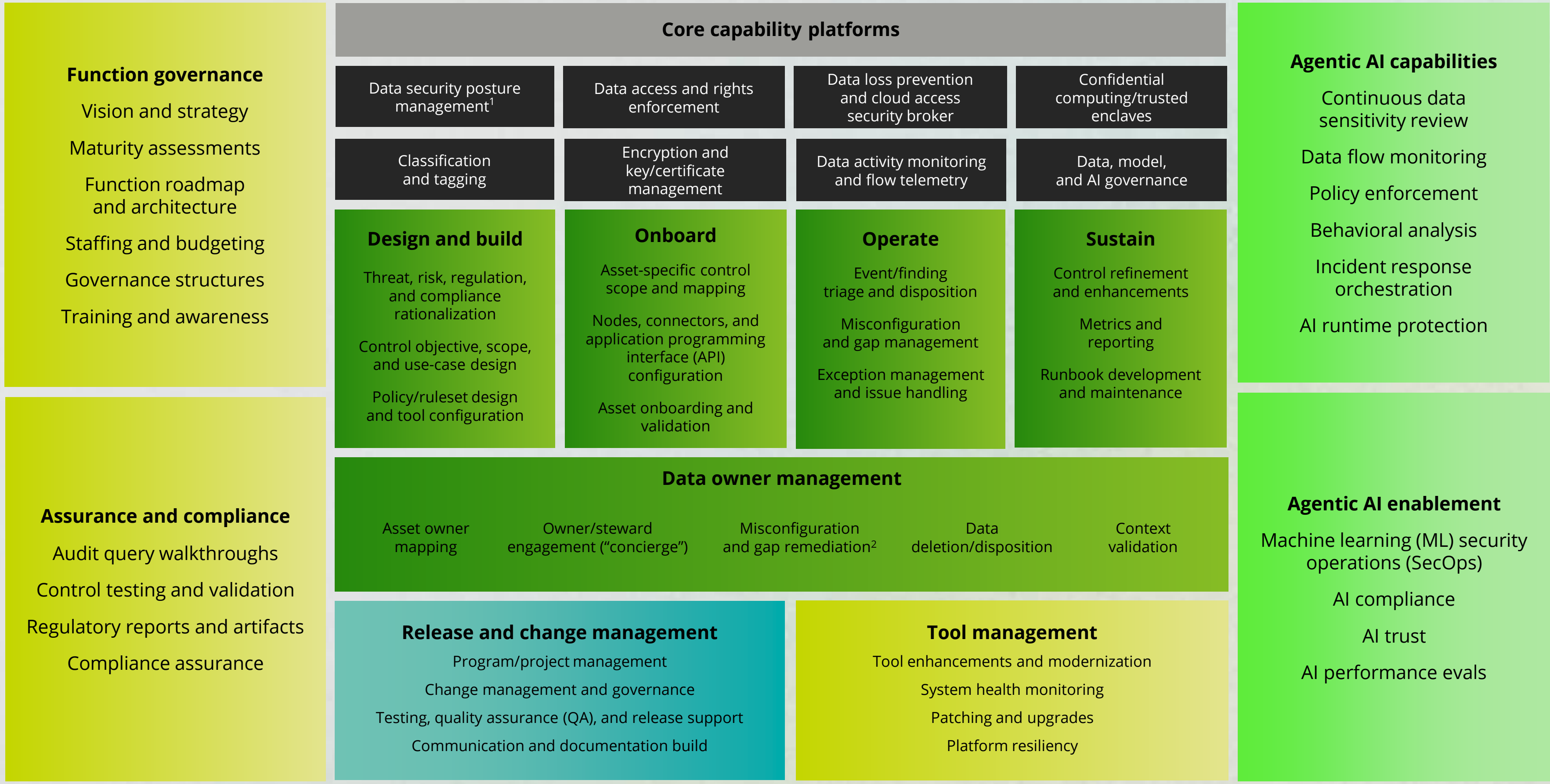
The explosive growth of enterprise data has fueled a rapid expansion of data services (platforms, data processing, and analytics). In this complex and ever-expanding data landscape, organizations need to tackle rising frequency and impact of breach events, further exacerbated by agentic artificial intelligence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

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.