



Reimagining the modern AI-enabled Secure by Design function

Rapid business demands are pushing organizations to develop and deploy applications promptly, often making it difficult to apply effective security throughout the process.

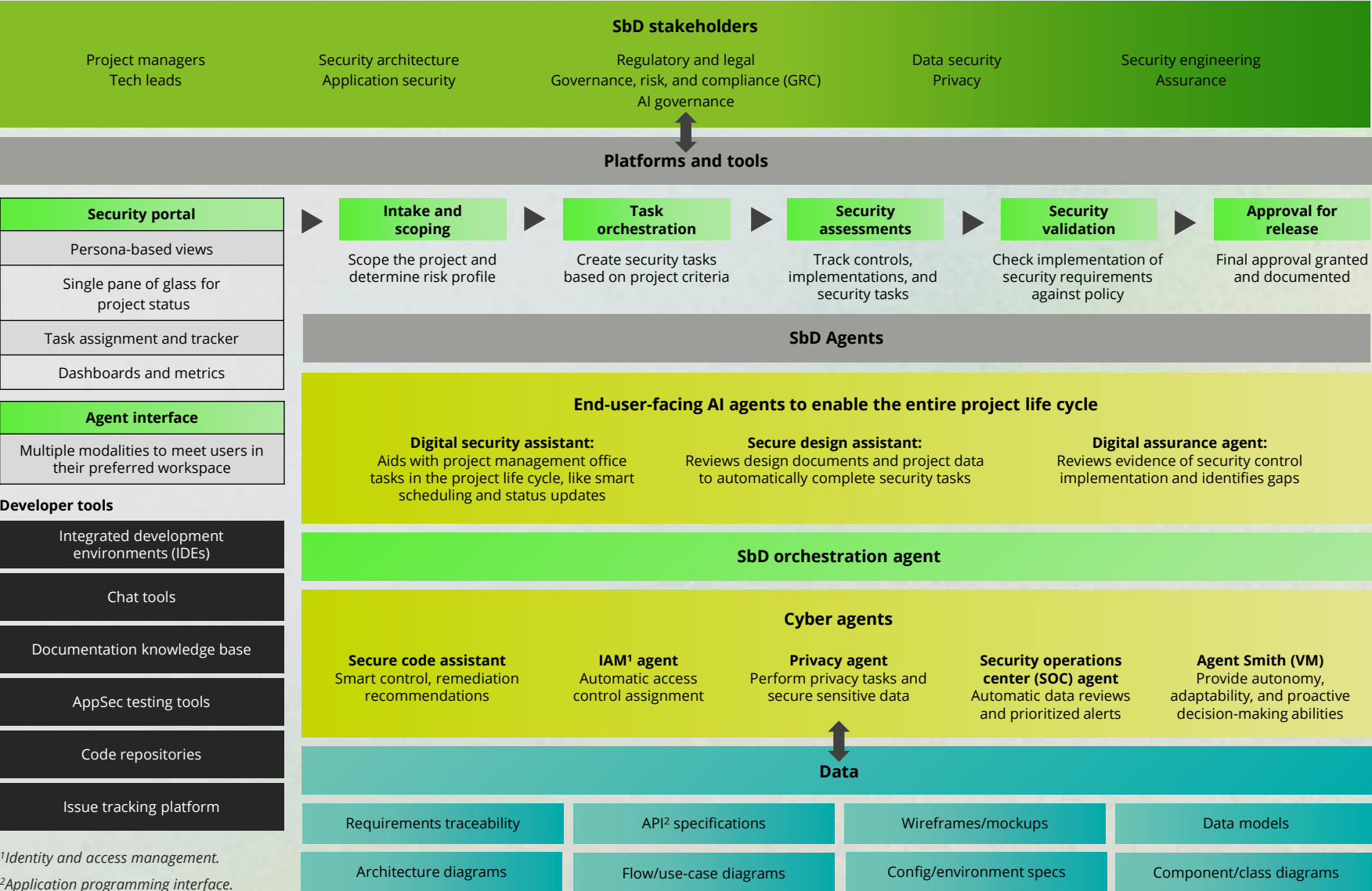
Secure by Design (SbD) is a security orchestration platform that centralizes security governance, automates security tasks, controls implementation, and integrates vulnerability management into the technology life cycle. This streamlines processes, reduces manual work, facilitates agile security, and improves compliance and efficiency.

Organizations often face inconsistent controls, siloed management, and manual processes, resulting in limited visibility and increased risk. SbD unifies and automates security practices to address these challenges.

Artificial intelligence (AI) further enhances security orchestration by reducing time spent on manual reviews, enabling broader insights into security compliance and controls, and integrating “smart” support to create a better user experience.

AI-driven SbD: Shaping tomorrow’s security

Securing the future: Agentic AI for SbD showcases a strategic, AI-powered approach to SbD, aligning stakeholders, platforms, and intelligent agents. By embedding agentic AI into security processes, organizations can streamline workflows, enhance collaboration, and strengthen defenses against evolving cyberthreats.



¹Identity and access management.

²Application programming interface.

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



Faris Naffaa
Senior Manager
Secure by Design Leader
Deloitte & Touche LLP
fnaffaa@deloitte.com



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

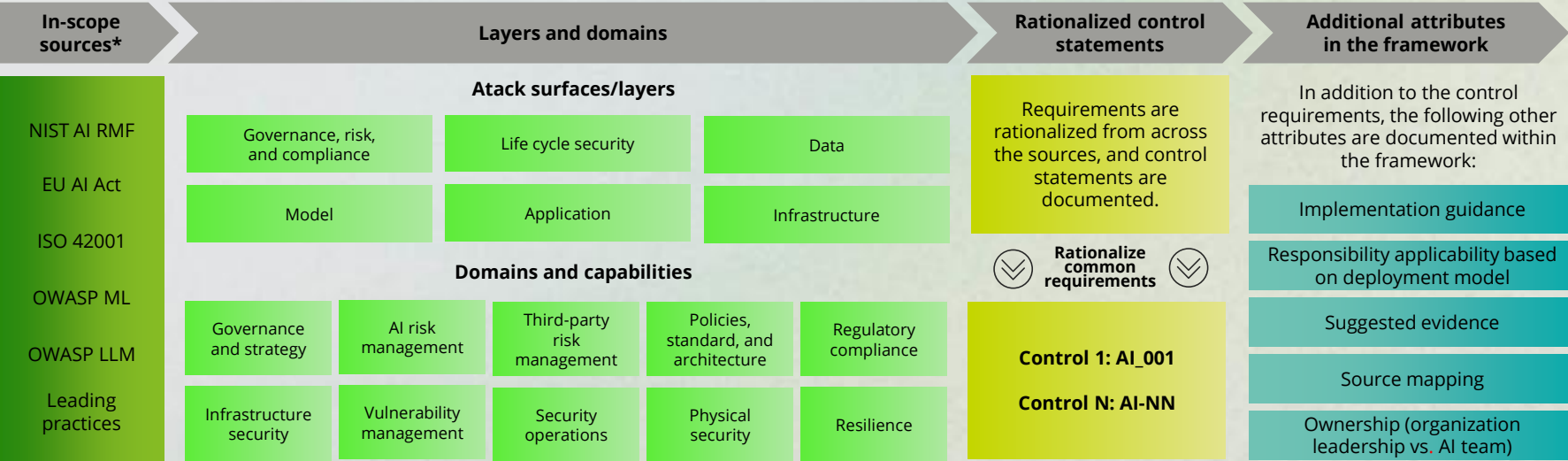
SbD is critical to secure AI applications

SbD involves integrating security mechanisms from the earliest stages of AI solution development. This means considering potential threats and mitigating risks during data collection, model design, deployment, and maintenance—not waiting until the end.

Proactive risk mitigation	Continued security integration	AI-centric security challenges	Regulatory and ethical compliance
Integrating security from the start enables early risk identification in the development life cycle. SbD principles are designed to reduce unnecessary features, permissions, or data exposures, thereby reducing opportunities for attackers.	SbD embeds security practices into each phase of development of IT projects, including AI assets. Automated security checks are used to continuously scan for vulnerabilities, misconfigurations, or compliance issues.	Model integrity: AI solutions are vulnerable to attacks; SbD helps protect model training. Auditability: Secure development practices make it easier to track changes, monitor access, and audit decisions for compliance and trust.	A SbD approach helps AI solutions meet compliance requirements by prioritizing security, generating evidence artifacts and live audit trails, and demonstrating to users, clients, and regulators that security is actively maintained and documented.

SbD for AI: Security controls framework

As organizations adopt AI, they may face risks like data privacy, bias, and security vulnerabilities. Deloitte’s AI security controls framework helps manage these risks and facilitates compliance with evolving AI regulations.



*Definitions: NIST AI RMF (National Institute of Standards and Technology AI Risk Management Framework); ISO (International Organization of Standardization); OWASP (Open Web Application Security Project); ML (machine learning); LLM (large language model)