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.

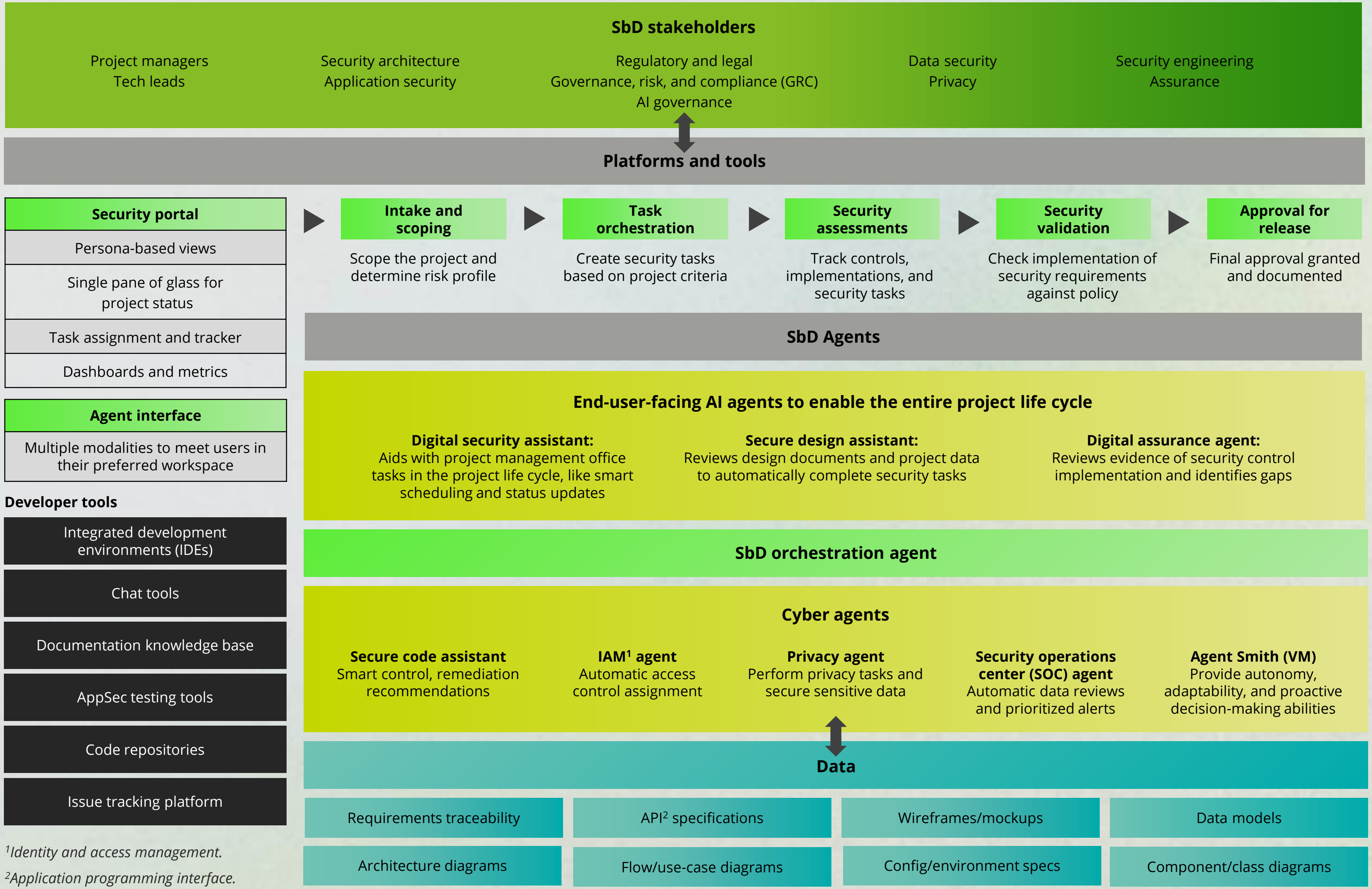
Secure by Design (SbD) is a security orchestration platform that centralizes security governance, automates security tasks, controls implementation, and integrates vulnerability management into the technology life cycle. This streamlines processes, reduces manual work, facilitates agile security, and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



SbD stakeholders

Project managers
Tech leads

Security architecture
Application security

Regulatory and legal
Governance, risk, and compliance (GRC)
AI governance

Data security
Privacy

Security engineering
Assurance

Platforms and tools

Security portal
- Persona-based views
- Single pane of glass for project status
- Task assignment and tracker
- Dashboards and metrics

Agent interface
- Multiple modalities to meet users in their preferred workspace

Developer tools
- Integrated development environments (IDEs)
- Chat tools
- Documentation knowledge base
- AppSec testing tools
- Code repositories
- Issue tracking platform

Intake and scoping: Scope the project and determine risk profile

Task orchestration: Create security tasks based on project criteria

Security assessments: Track controls, implementations, and security tasks

Security validation: Check implementation of security requirements against policy

Approval for release: Final approval granted and documented

SbD Agents

End-user-facing AI agents to enable the entire project life cycle

Digital security assistant: Aids with project management office tasks in the project life cycle, like smart scheduling and status updates

Secure design assistant: Reviews design documents and project data to automatically complete security tasks

Digital assurance agent: Reviews evidence of security control implementation and identifies gaps

SbD orchestration agent

Cyber agents

Secure code assistant
Smart control, remediation recommendations

IAM[1] agent
Automatic access control assignment

Privacy agent
Perform privacy tasks and secure sensitive data

Security operations center (SOC) agent
Automatic data reviews and prioritized alerts

Agent Smith (VM)
Provide autonomy, adaptability, and proactive decision-making abilities

Data

- Requirements traceability
- API[2] specifications
- Wireframes/mockups
- Data models
- Architecture diagrams
- Flow/use-case diagrams
- Config/environment specs
- Component/class diagrams

[1] *Identity and access management.*

[2] *Application 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

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.

Continued security integration

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.

AI-centric security challenges

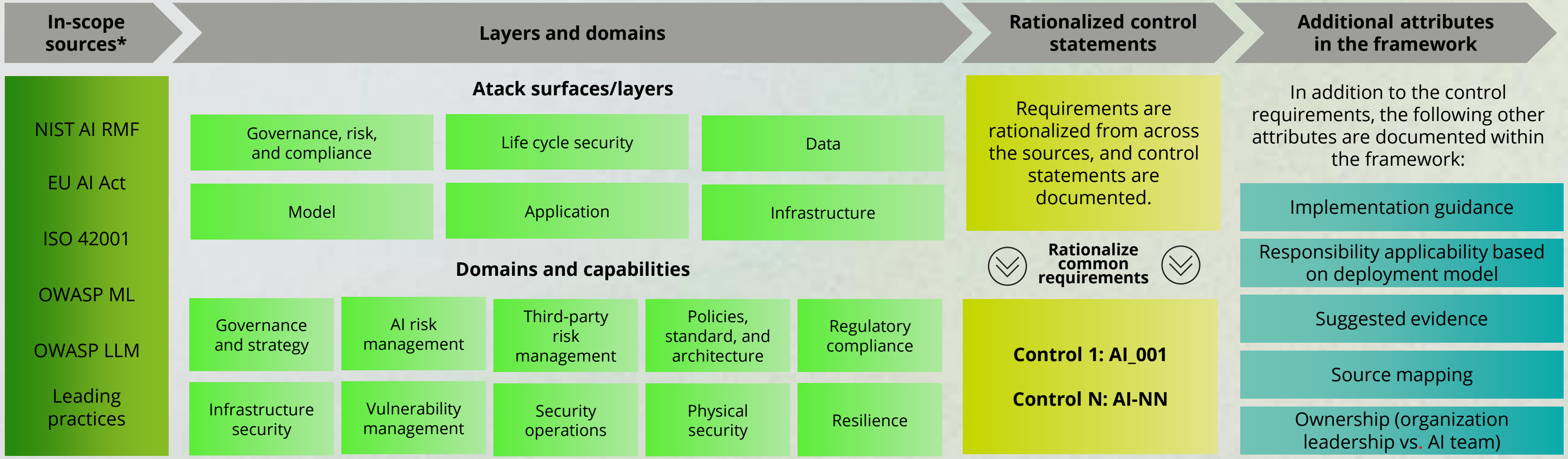
Model integrity: AI solutions are vulnerable to attacks; SbD helps protect model training. **Auditability:** Secure development practices make it easier to track changes, monitor access, and audit decisions for compliance and trust.

Regulatory and ethical compliance

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.



In-scope sources*

NIST AI RMF
EU AI Act
ISO 42001
OWASP ML
OWASP LLM
Leading practices

Layers and domains

Atack surfaces/layers

Governance, risk, and compliance
Life cycle security
Data
Model
Application
Infrastructure

Domains and capabilities

Governance and strategy
AI risk management
Third-party risk management
Policies, standard, and architecture
Regulatory compliance
Infrastructure security
Vulnerability management
Security operations
Physical security
Resilience

Rationalized control statements

Requirements are rationalized from across the sources, and control statements are documented.

Rationalize common requirements

Control 1: AI_001

Control N: AI-NN

Additional attributes in the framework

In addition to the control requirements, the following other attributes are documented within the framework:

Implementation guidance
Responsibility applicability based on deployment model
Suggested evidence
Source mapping
Ownership (organization leadership vs. AI team)

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)

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.