

# Elevating cyber protections with Secure by Design

Business requirements and customer demands are forcing organizations to rapidly develop and deploy applications and bring products to market.

This expedited development and expansion introduces a multitude of challenges when it comes to applying security:

**Difficulty applying consistent and standardized security controls** across all solutions in the product lifecycle.

**Security is managed in a siloed manner** and may be implemented differently across teams, making it difficult to scale security operations across the development process.

Hard security gate-checks cause strain amongst the business, development, and security teams and can become a blocker to deployment, making security look like a burden rather than an enabler for development teams.

**Lack of end-to-end visibility of security posture** and security control implementation across the application and product lifecycle.

#### Secure by Design can help organizations:

- Bring ubiquity and agility to the end-to-end development process.
- Make security consumable to the business.
- Enable centralized reporting to provide visibility into security metrics and risk posture.
- Standardize security controls across the organization, and automate the generation and validation of security requirements.

#### Foundations of Secure by Design

Secure by Design's workflows occur throughout the Secure Software Development Lifecycle (SSDLC) process and across multiple business teams. It leverages automation to generate and assign security tasks in addition to prescribing security controls based on one form completed by the customer.



#### Intake

Provide one intake form for all new IT projects

Secure by Design leverages a standardized intake form for all security domains to identify the scope, inherent risk, and project requirements. A record is created to track all pre-production security activity and outcomes throughout its lifecycle.

2

#### **Task creation**

Create and assign security tasks

Tasks across multiple security domains should be prioritized based on risk and centrally managed to enable transparency and tracking.

#### **Security Teams**

- Data security
- Privacy
- Vendor risk
- Application security
- Security architecture

3

#### **Security assessments**

Execute requirements across multiple security domains

The assessment framework and methodology should be standardized and mapped to a defined Control Library.

#### Assessments

- Security architecture review
- Threat modeling
- Data security & orivacy review
- Vulnerability testing
- Vendor risk

# 4

#### **Security validation**

Validate against requirements and policy

Validation of requirement fulfillment and control implementation should be based on risk and predefined by policy. Secure by Design leverages policy-as-code to automate policy checks and compliance-as-code to automate overall compliance to automate and reduce user error while validating.

# 5

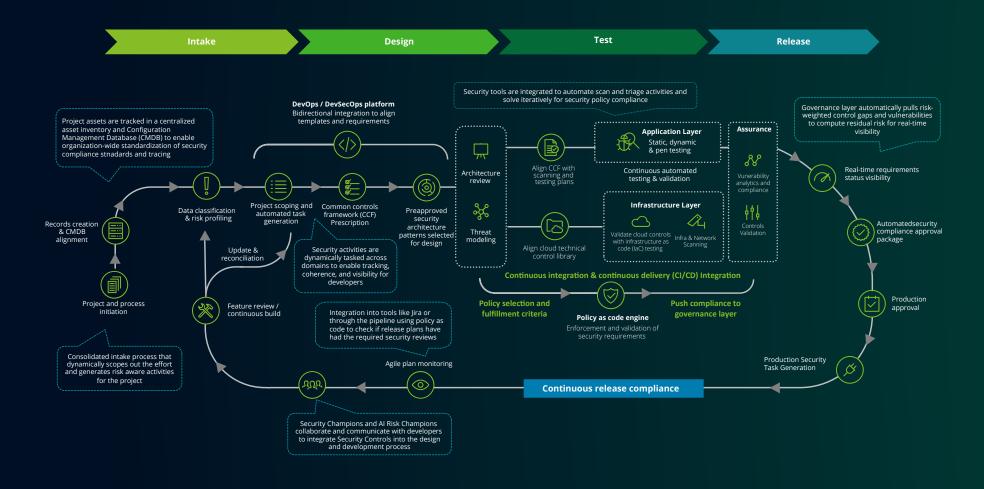
#### **Approval for release**

Review and approve prior to granting Authority-to-Operate (ATO)

Approval is granted for release after reviewing and validating the implemented security controls against requirements defined for each project during the Secure by Design lifecycle. Approvals should be manually enforced through review boards/toll gates and automated in deployment pipelines.

#### Workflow

Powered by automated governance and accountability layers, the following workflow depicts an ideal and mature approach to achieving end-to-end security across the entire IT lifecycle from the planning and ideation phase through the production state and beyond.



#### **Success Story**

# Security automation

#### **Fortune 50 Hospitality Client**

To better secure its Software Development Lifecycle (SDLC) and enhance its cybersecurity posture, this client engaged Deloitte to build and operationalize a robust automation solution that supported multiple development environments and methodologies, rooted within the SDLC and integrated with project management tools.

- Codified security controls and mapped to security assessment results for automated control generation
- Integrated application testing tools with CI/CD pipeline, pattern provisioning, bug tracking tool, and deployment process
- Implemented automated workflow management for tracking and approval of security requirements based on risk classifications
- Integrated with project management solution to provide demand

#### **Outcomes**

- Operationalized Threat Modeling team
- Automated onboarding, security scan execution, and triaging
- Security automation integrated into SDLC
- Robust dashboards and reporting

Unlock the full power of Secure by Design. Let us show you how.



Adnan Amjad

Partner

US Cyber Offering Portfolio Leader Deloitte & Touche LLP

<u>aamjad@deloitte.com</u>



Vikram Kunchala

<u>Principal</u>

US Cyber Solutions and Platforms Leader

Deloitte & Touche LLP

vkunchala@deloitte.com



Faris Naffaa

Senior Manager

Secure by Design Solution Leader Deloitte & Touche LLP

fnaffaa@deloitte.com

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 adviser. 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.